¡Completamente revisado y actualizado!



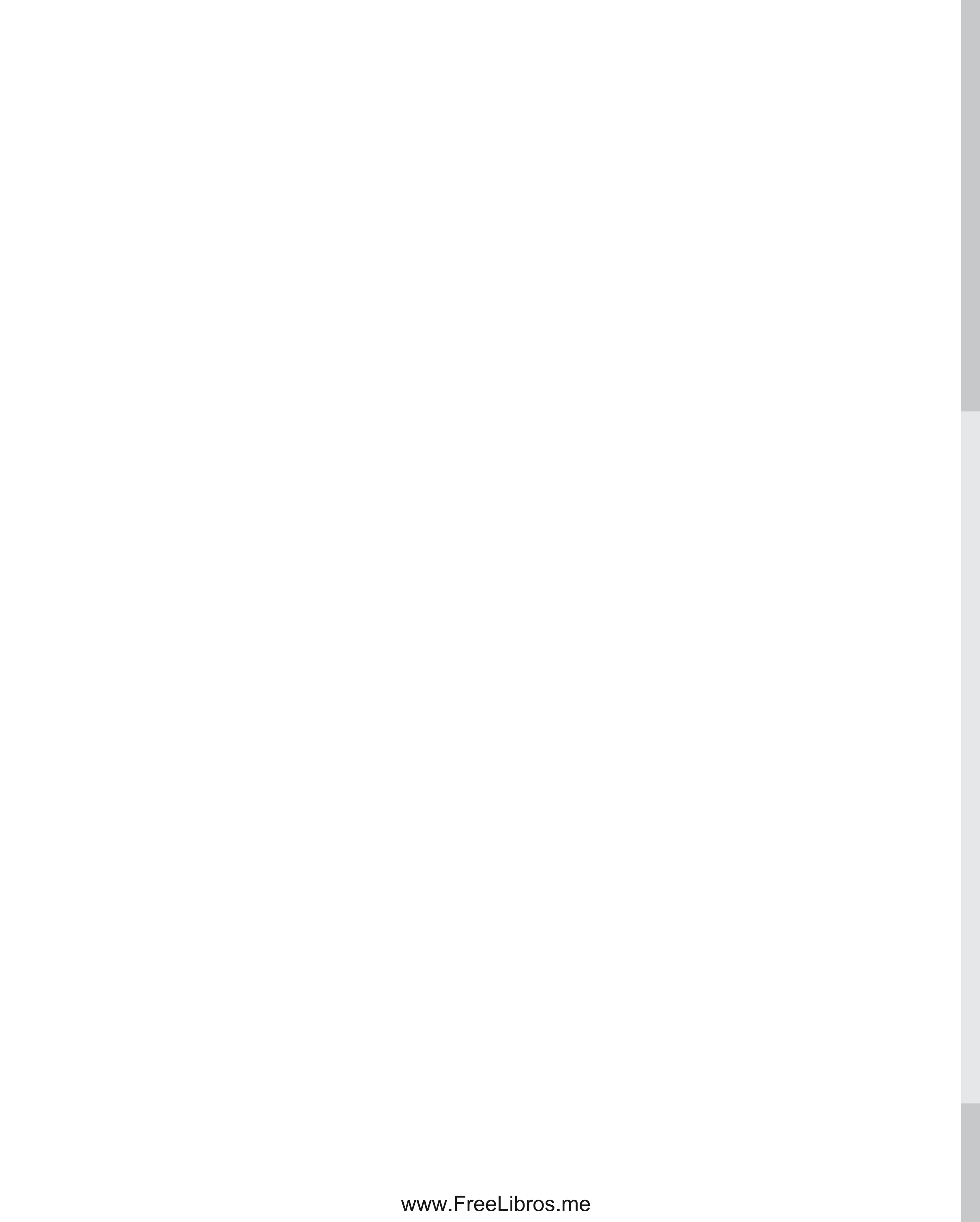
FUNDAMENTOS DE REDES

Bruce A. Hallberg

Cuarta edición

- Aprenda los fundamentos de la conectividad de las redes cableadas e inalámbricas, que incluyen diseño, configuración, hardware y seguridad.
- Trabaje con protocolos de red TCP/IP, DHCP, VoIP y otros.
- Utilice las tecnologías de acceso remoto más recientes, entre ellas, SSL VPNs.
- Aprenda las instrucciones paso a paso para la instalación y administración de Windows Server 2003, Windows 2000 Server, Linux y Apache.

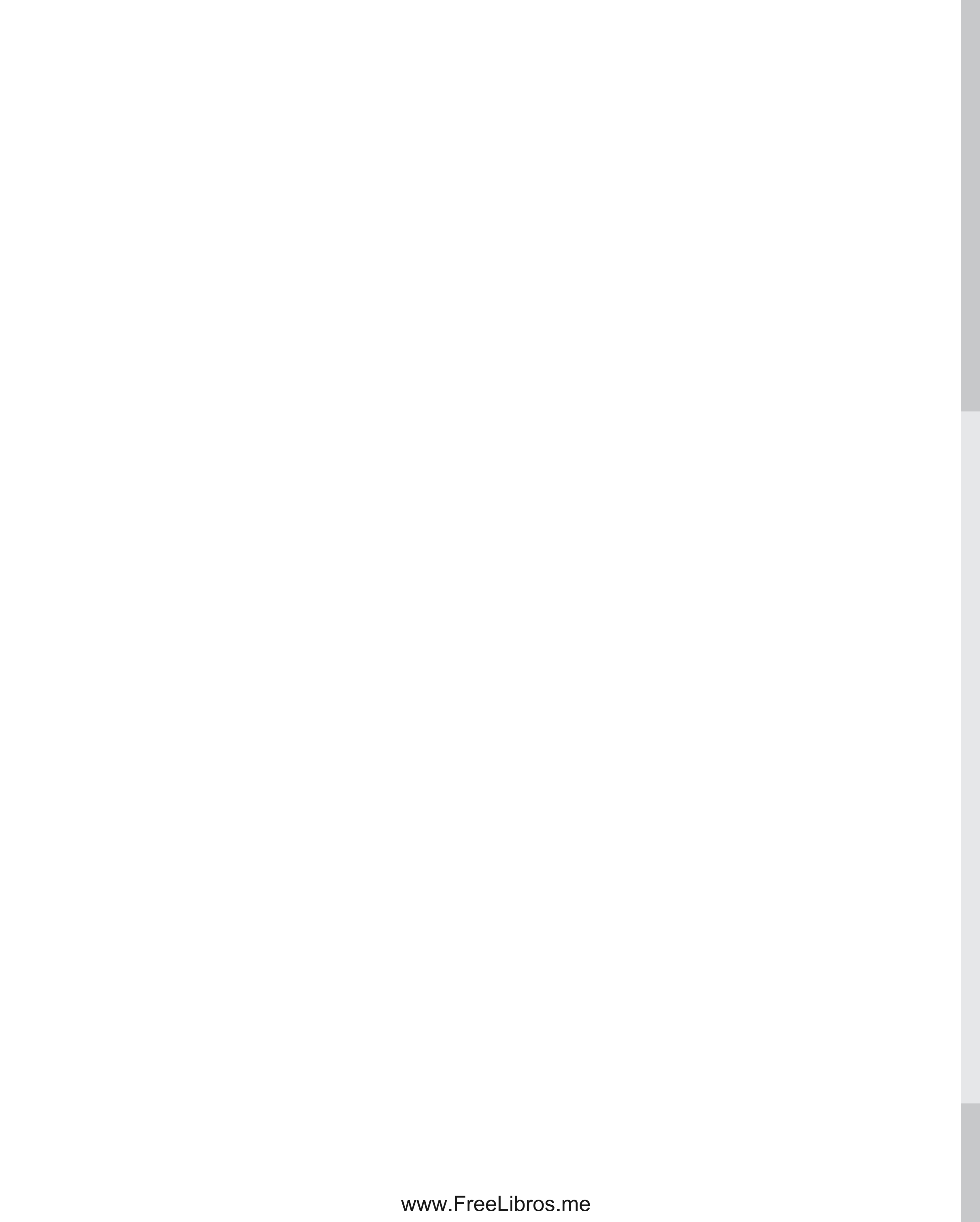






Fundamentos de redes

4ª. edición



Fundamentos de redes
4ª. edición

BRUCE **HALLBERG**

Traducción

Carlos Roberto Cordero Pedraza

Catedrático

Secretaría de Marina y Armada de México, CESNAV



MÉXICO • BOGOTÁ • BUENOS AIRES • CARACAS • GUATEMALA • LISBOA
MADRID • NUEVA YORK • SAN JUAN • SANTIAGO • AUCKLAND • LONDRES
MILÁN • MONTREAL • NUEVA DELHI • SAN FRANCISCO • SAO PAULO
SINGAPUR • ST. LOUIS • SYDNEY • TORONTO

Gerente de división: Fernando Castellanos Rodríguez
Editor de desarrollo: Cristina Tapia Montes de Oca
Supervisor de producción: Jacqueline Brieño Álvarez

Fundamentos de redes. 4ª. edición



*A Subsidiary of **The McGraw-Hill** Companies, Inc.*
Corporativo Punta Santa Fe
Prolongación Paseo de la Reforma 1015, Torre A
Piso 17, Colonia Desarrollo Santa Fe
Delegación Álvaro Obregón
C.P. 01376, México, D.F.
Miembro de la Cámara Nacional de la Industria Editorial Mexicana, Reg. Núm. 736

ISBN 970-10-5896-8

Translated from the fourth English edition of
NETWORKING A BEGINNER'S GUIDE
By: Bruce Hallberg

ISBN: 0-07-226212-5

1234567890 0987543216

Impreso en México *Printed in Mexico*

The McGraw-Hill Companies

Para Hill
y Debbie Scherrer,
mis suegros,
con amor y admiración

ACERCA DEL AUTOR

Bruce Hallberg ha trabajado en la industria de la computación por más de veinte años y ha sido consultor de las 1 000 compañías de *Fortune* sobre la implantación de sistemas de administración de información y de conectividad.

Acerca del editor técnico

James F. Nelly trabaja en la actualidad como escritor técnico por su cuenta en Atlanta, Georgia. Jim se graduó de la Florida State University con una licenciatura en Ciencias en Ingeniería Industrial y de la University of West Florida con una licenciatura en Artes en Inglés. Ha trabajado en empresas de tecnología por más de nueve años, tiempo durante el cual ha proporcionado ayuda a clientes con varios proyectos a la vez que ofrece servicios de consultoría sobre nuevas tecnologías.

UN VISTAZO AL CONTENIDO

Parte I Fundamentos de la conectividad de redes

Parte II Conocimiento por medio de la práctica

CONTENIDO



RECONOCIMIENTOS

Libros como éste no se concretan por medio de los esfuerzos de una sola persona, sino de todo un grupo de ellas. Quisiera llamar su atención sobre las siguientes personas por sus contribuciones.

Jane Brownlow fue editora ejecutiva de esta cuarta edición de Fundamentos de redes. Ella se encargó de concretar el concepto inicial y su estructura, consiguió la aprobación del director editorial a fin de avanzar en el proyecto, administró todos los problemas contractuales y dirigió el libro hasta su terminación. Asimismo, Jane fue la editora de adquisiciones de la primera edición de este libro y, además, responsable en gran medida de su concepto inicial. He trabajado con Jane un gran número de años y es, sin lugar a dudas, la editora de adquisiciones más dedicada, profesional y perseverante con la que jamás haya trabajado.

Jennifer Housh fue coordinadora de adquisiciones de este libro, responsable de asegurar de que todas sus partes se coordinaran y de enviar los diferentes capítulos a las personas que necesitaban trabajar con ellos. Sin los esfuerzos de Jenni, el proyecto pudo haber sido caótico.

Jim Kelly se encargó de la edición técnica de esta obra. Jim verificó con mucho cuidado la precisión de todo el material técnico. Además, en las áreas en las que se proporcionaban instrucciones paso a paso, los llevó a cabo en su totalidad a fin de asegurarse de que funcionarán de la manera que se menciona. También fueron de mucha ayuda sus sugerencias sobre temas adicionales que se debían cubrir o mencionar, con lo cual hizo un trabajo estupendo.

Emily Rader se encargó de la corrección de este libro. En realidad no puedo decir sino cosas muy agradables respecto a Emily. Éste es el segundo proyecto en el que trabajo con ella. Tiene un toque muy atinado en su labor de corrección, nunca se le escapa un error; es un placer trabajar con ella.

Sam se encargó de la tarea de editar el libro. Dicha tarea incluye trabajar con los correctores y producción a fin de llevar el libro a su término. Sam fue muy competente y profesional.

Por último, sería en verdad negligente de mi parte si no mencionara a mi familia por haber soportado mi ausencia durante tres meses. Muy en particular, quisiera agradecer a mi esposa, Christy: su ayuda en verdad hizo posible que trabajara en este libro.

INTRODUCCIÓN

He consultado a muchas personas durante años, las cuales tienen un gran —incluso impresionante— conocimiento práctico sobre PC, sistemas operativos, aplicaciones y problemas y soluciones comunes. La mayoría de ellas son gurús con las computadoras de escritorio. Sin embargo, muy pocas han sido capaces de hacer la transición de trabajar con las redes, y han tenido problemas para obtener el conocimiento suficiente para conceptualizarlas, comprenderlas, instalarlas, administrarlas y repararlas. En muchos casos, esta falta de capacidad limita su desarrollo profesional debido a que gran parte de las compañías consideran que poseer experiencia en la conectividad de redes es fundamental para alcanzar posiciones de alto nivel en el campo de las tecnologías de la información (TI). Y, en realidad, la experiencia en el campo de la conectividad de redes es muy importante.

Es cierto que las redes pueden ser bestias complicadas que se tienen que aprender. Para empeorar las cosas, la mayoría de las empresas no están en posición de dejar que empleados que carecen de destrezas con las redes experimenten y aprendan sobre ellas utilizando la red de producción de la compañía. Esto deja al principiante en este campo en la difícil posición de tener que aprender acerca de las redes mediante:

- Lectura de un número interminable de libros y artículos
- Asistencia a clases
- Construcción de pequeñas redes experimentales en casa, utilizando partes y software de desecho o prestado

Este libro está diseñado para gente versada en computadoras y en los fundamentos de la ciencia de la computación, pero que, sin embargo, desean obtener mayor educación acerca de redes y conectividad. Supongo que comprende y está familiarizado con los temas siguientes:

- Cómo funcionan los bits y bytes.
- Nociones de la notación binaria, octal, decimal y hexadecimal.
- Funcionamiento del hardware básico de la PC e instalación y reemplazo de los componentes periféricos de la PC. Usted deberá conocer qué son las IRQ, DMA y las direcciones de memoria.
- Dos o tres sistemas operativos de escritorio con detalle, como Windows, Macintosh, Linux o Unix y, quizás, DOS.
- Un conocimiento detallado de una amplia variedad de software de aplicación.

El propósito de este libro es tanto educar como familiarizar. En la primera parte se analiza la tecnología y el hardware básico de conectividad de redes. Su propósito es ayudarlo a comprender los componentes básicos de la conectividad, de forma que pueda construir un marco conceptual en el cual pueda colocar el conocimiento más detallado en su área de especialización. La segunda parte se avoca a familiarizarlo con los tres sistemas operativos de red más importantes: Windows 2000 Server, Windows Server 2003 y Linux. En ella aprenderá los fundamentos de la instalación y administración de dichos sistemas operativos de red.

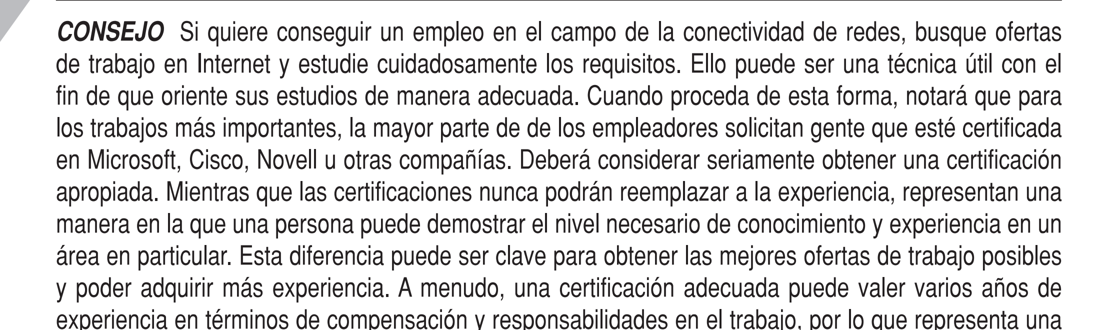
El objetivo de este libro es servir como un trampolín a partir del cual pueda comenzar a adquirir un conocimiento más detallado en las áreas de su interés. A continuación se presentan algunas ideas acerca de las áreas en las que podría estar interesado en continuar explorando, en función de sus objetivos profesionales:

- **Administrador de redes pequeñas a medianas** Si planea construir y administrar redes con 200 o menos usuarios, debe ampliar sus conocimientos mediante el estudio de los sistemas operativos de red que piensa utilizar, el hardware del servidor, la administración de la PC cliente y la administración de la red. Podría ser que encontrara información más detallada sobre el hardware de la red, como ruteadores, puentes, compuertas, switches y temas por el estilo que le fueran útiles, pero probablemente podría no tener importancia para usted.
- **Administrador de una red grande** Si planea trabajar con redes de más de 200 usuarios, necesita obtener un conocimiento detallado acerca del direccionamiento y enrutamiento TCP/IP y del hardware de la red que incluyan ruteadores, puentes, compuertas, switches y paredes. Asimismo, en redes de gran tamaño, los administradores tienden a especializarse en ciertas áreas, por lo que debe considerar algunas áreas de especialización en particular, como servidores de e-mail como Lotus Notes o Microsoft Exchange, o servidores de bases de datos como Oracle o SQL Server.
- **Administrador de Internet** En estos días muchas personas estudian especialidades en tecnologías basadas en Internet. En función del área en la que desee trabajar, deberá aprender más acerca de los servidores web y FTP, http y otros protocolos de Internet a nivel aplicación, CGI y otras tecnologías de escritura web, diseño en HTML



y conexiones de correo SMTP. Probablemente que desee convertirse en un experto en TCP/IP y todos sus protocolos relacionados, reglas de direccionamiento y técnicas de enrutamiento.

- **Soporte del usuario final** Si su trabajo principal es proporcionar soporte a los usuarios finales, quizá con soporte de cómputo de aplicación o cliente, se puede beneficiar de un conocimiento más profundo de la conectividad de redes. Las aplicaciones de cómputo cliente generalmente interactúan con la red y la comprensión de las redes sin duda le ayudará a ser más eficiente.

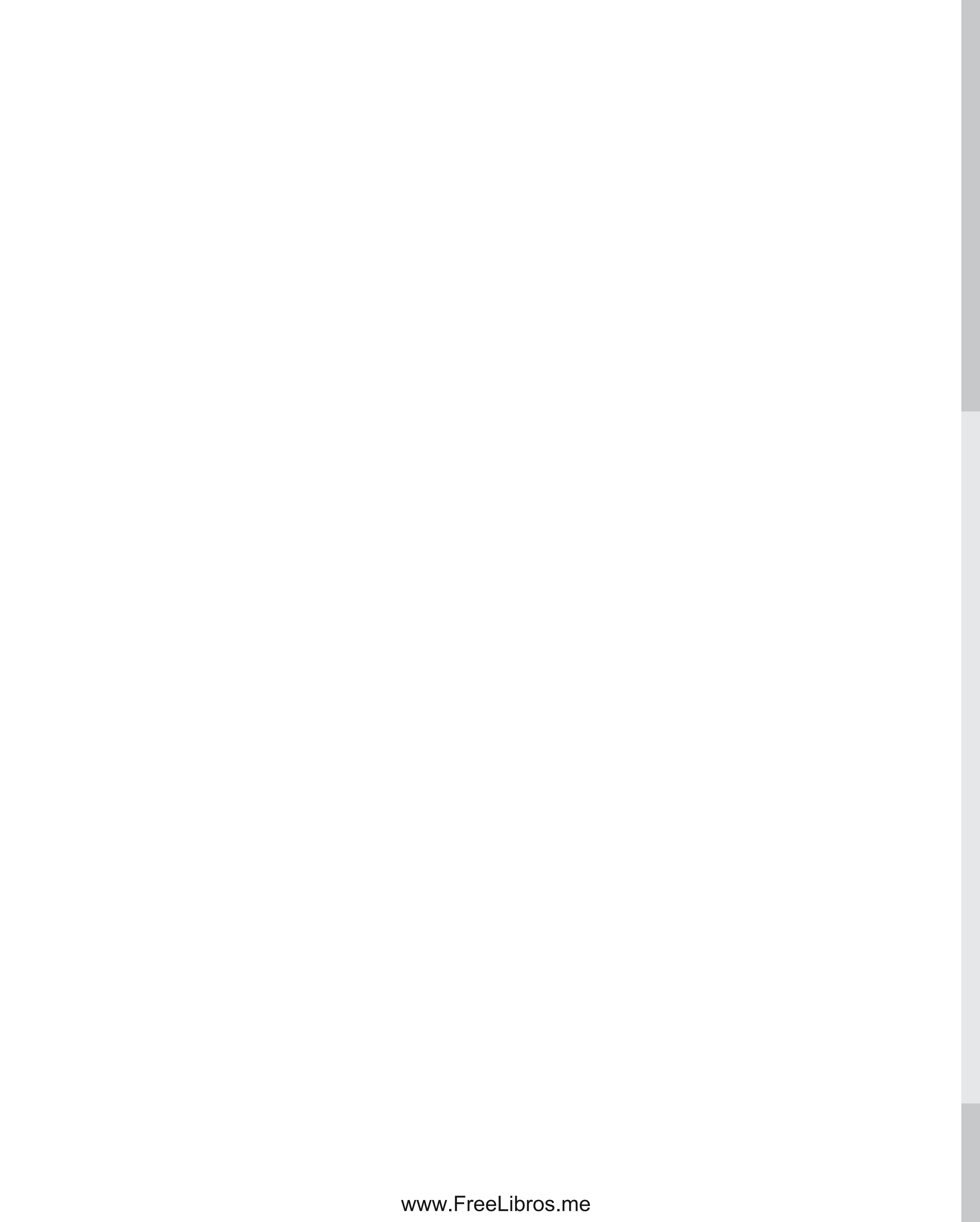


CONSEJO Si quiere conseguir un empleo en el campo de la conectividad de redes, busque ofertas de trabajo en Internet y estudie cuidadosamente los requisitos. Ello puede ser una técnica útil con el fin de que oriente sus estudios de manera adecuada. Cuando proceda de esta forma, notará que para los trabajos más importantes, la mayor parte de de los empleadores solicitan gente que esté certificada en Microsoft, Cisco, Novell u otras compañías. Deberá considerar seriamente obtener una certificación apropiada. Mientras que las certificaciones nunca podrán reemplazar a la experiencia, representan una manera en la que una persona puede demostrar el nivel necesario de conocimiento y experiencia en un área en particular. Esta diferencia puede ser clave para obtener las mejores ofertas de trabajo posibles y poder adquirir más experiencia. A menudo, una certificación adecuada puede valer varios años de experiencia en términos de compensación y responsabilidades en el trabajo, por lo que representa una inversión en usted mismo que generalmente se recupera en un corto periodo.



PARTE I

Fundamentos de la conectividad de redes



CAPÍTULO 1

El negocio de la conectividad

Este libro es una guía de principio a fin para el principiante en conectividad de redes. Antes de ir a los bits y bytes, temas que se estudian en el resto del texto, usted debe comprender los porqué y para qué de la conectividad. Este capítulo estudia la conectividad de redes desde una perspectiva de negocios. Aprenderá acerca de los beneficios que proporciona la conectividad a una compañía y los diferentes tipos de trabajos disponibles en este campo. Asimismo, descubrirá cómo se les proporciona soporte a las redes desde la perspectiva de negocios y cómo puede empezar una carrera en la conectividad de redes. Por último, aprenderá acerca de la ley Sarbanes-Oxley de 2002 y cómo afecta los requisitos exigidos a los profesionales de la conectividad.

CONECTIVIDAD DE REDES: LA PERSPECTIVA CORPORATIVA

Para ser realmente eficiente en el campo de la conectividad de redes, necesita comenzar por conocer el tema desde una perspectiva corporativa. ¿Por qué son importantes las redes para las compañías? ¿Qué función llevan a cabo para ellas? ¿De qué formas los profesionales de la conectividad satisfacen las necesidades de la compañía con las redes que instalan y mantienen? Es importante darse cuenta de que no existe una respuesta única y correcta. Cada compañía tiene diferentes necesidades y expectativas respecto a sus redes. Lo importante es que conozca las preguntas que se deben hacer respecto a la conectividad de redes y plantear las mejores respuestas posibles para su compañía. Llevar a cabo lo anterior asegurará que la red de su compañía satisfaga de una manera óptima sus necesidades.

¿Qué necesita su compañía?

Existen muchas posibles razones por las cuales una compañía necesite o se beneficie de una red. Con la finalidad de comprender su compañía, usted debe comenzar por analizar las preguntas siguientes. Cuestione a una gran variedad de miembros de la compañía su perspectiva respecto de esas preguntas: entre los directivos deben estar el director general o propietario de la compañía, el director de finanzas y los jefes de varios departamentos clave, como los de manufactura, ventas y mercadotecnia, contabilidad, adquisiciones y materiales, etc. La gama de ejecutivos que tendrá que entrevistar dependerá del tipo de negocio en el que la compañía esté involucrada.

Es importante que comience por comprender el negocio y las perspectivas orientadas al negocio de estos ejecutivos y sus departamentos. Tome en cuenta las preguntas siguientes en cada área clave:

- ¿Cuál es su función en la compañía?
- ¿De qué manera coinciden sus objetivos con los de la compañía?
- ¿Cuáles son las metas clave de su función el próximo año? ¿Qué hay acerca de los próximos cinco años?
- ¿Cuáles consideran los retos más importantes por enfrentar para lograr sus metas?

- ¿De qué forma la tecnología de información (TI) juega un papel importante para lograr sus objetivos?
- ¿Qué tipo de automatización les ayudará a alcanzar sus objetivos?
- ¿Cómo se lleva a cabo el trabajo en sus áreas? Por ejemplo, ¿la mayoría de su personal realiza trabajo mecánico, como en una línea de producción, o son "trabajadores del conocimiento", los cuales generan documentos, analizan información, etcétera?

Su objetivo al formular estas preguntas, y otras que se le puedan ocurrir, es obtener una idea clara de cada área funcional: qué hace y cómo lo hace, así como de qué desea ser capaz en el futuro. Una vez que haya comprendido lo anterior, usted puede analizar el efecto que la red —las mejoras a la red existente— tendrá en las diferentes áreas de la compañía.

Comenzar desde una perspectiva de negocios es absolutamente esencial. Las redes no se construyen y se actualizan "no más porque sí", la actualización de una de ellas necesita estar supeditada a las necesidades del negocio. La justificación para instalar una red, o actualizar una existente, deberá mostrar de manera clara la forma en que ayudará al funcionamiento correcto del negocio, o de qué manera jugará un papel importante para el logro de los objetivos de la compañía, que tendrán que ser congruentes con el costo y los esfuerzos que conlleven.

Después de tener una comprensión total de la compañía, sus objetivos y la forma en que lleva a cabo sus procesos, podrá analizar las diferentes ideas que pueda tener para la red y cómo beneficiarán a algunas o a todas las partes del negocio. Para hacer esto, necesitará considerar al menos las áreas siguientes:

- ¿Existe algún área en la que la falta de una red o alguna falla en la red existente obstaculiza a la compañía para alcanzar sus metas o elaborar su trabajo? Por ejemplo, si una red existente se diseñó sin la capacidad adecuada y esto provoca que el personal pierda demasiado tiempo en las tareas rutinarias (como guardar o enviar archivos o compilar programas), ¿qué mejoras deberán hacerse para solucionar esos problemas? También puede ser que la red y sus servidores no sean confiables, por lo que los empleados a menudo pierden trabajo o están improductivos mientras se resuelven los problemas.
- ¿Existen mejoras que pudieran adicionarse a la red a fin de que proporcionara beneficios al negocio? Por ejemplo, si muchas personas de la compañía envían faxes con demasiada frecuencia (como el personal de ventas que envía cotizaciones a clientes), ¿agregar un sistema de fax en la red produciría beneficios en cuanto a la productividad? ¿Qué hay respecto a otras aplicaciones de la red? (En el capítulo 3 se presentan algunas características comunes de las redes que probablemente desee revisar para responder estas preguntas).
- ¿Qué otros planes de automatización existen que requieran el soporte de la red? Por ejemplo, digamos que usted es el administrador de la red de una compañía. ¿Qué aplicaciones o características novedosas se agregarán a la red a la que usted necesita proporcionar soporte? ¿Planea la compañía instalar algún tipo de sistema de videoconferencia, por ejemplo? Si es así, ¿conoce usted qué cambios necesitará llevar a cabo en la red a fin de dar soporte al sistema?
- ¿Qué se necesita hacer a la red simplemente para darle mantenimiento? En la mayoría de las compañías, los requerimientos de espacio en archivo crecen de manera muy rápida, aun si el negocio en sí no se encuentra en expansión. ¿Cuánto espacio de almacenamiento adicional necesita la red para mantenerse en operación sin problemas? ¿Cuántos

servidores adicionales y otras cosas se van a necesitar para mantener a la red trabajando debidamente?

Es obvio que una lista como la anterior no puede ser exhaustiva. Lo importante es que usted necesita resolver el problema de la conectividad de la red primero desde una perspectiva de la compañía y de sus necesidades. Dentro de ese marco, utilice su creatividad, conocimiento, experiencia e ingenio para proponer y ejecutar un plan para la red. En lo que resta de este libro se analiza la información que necesita para aprender acerca de esta importante parte de la infraestructura de cualquier compañía.

PUESTOS DE TRABAJO EN LA CONECTIVIDAD DE LAS REDES

Si planea ingresar al campo de la conectividad de redes (y si está leyendo este libro, seguramente lo hace), es importante tener una idea de los diferentes puestos de trabajo que encontrará y de los que típicamente requerirá. Por supuesto, los requerimientos reales de los puestos de trabajo variarán ampliamente de compañía a compañía dependiendo de las diferentes redes instaladas. Asimismo, las diferentes empresas pueden tener oportunidades con las cuales puede empezar una carrera en el campo de la conectividad de redes. Una vez dicho lo anterior, las descripciones siguientes presentan un amplio panorama de algunos puestos de trabajo clave.

Administrador de red

Los administradores de red son responsables de las operaciones de la misma red o, en compañías grandes, de las operaciones de las partes clave de una. En una compañía pequeña en la que solamente existe un administrador de red, se incluyen las tareas siguientes:

- Crear, mantener y eliminar cuentas de usuario.
- Asegurarse de que se realicen los respaldos necesarios de manera regular.
- Administrar las "claves" de la red, como las cuentas administrativas y sus contraseñas.
- Administrar las políticas de seguridad de la red.
- Agregar nuevo equipo de conectividad, como servidores, ruteadores, concentradores y switches, y administrarlo.
- Supervisar la red, tanto el hardware como el software, para detectar problemas potenciales y los niveles de utilización a fin de realizar la planeación de las actualizaciones de la misma.
- Reparar los problemas de la red (generalmente ¡lo más rápido posible!).

Los administradores de la red podrían también llamarse administradores de sistemas, de LAN y otras variaciones sobre el mismo tema.

Típicamente usted debe contar con varios años de experiencia en tareas relacionadas con una red similar para realizar este trabajo. Las certificaciones como la Microsoft Certified Systems Engineer (MCSE), la Microsoft Certified Systems Administrador (MCSA) o la Certified Novell Engineer de

Novell (CNE) pueden reducir la cantidad de experiencia que las compañías suelen requerir. Por lo general, las empresas consideran que estas certificaciones son importantes ya que aseguran que el candidato reúne un mínimo de requisitos para instalar u operar el sistema de conectividad en cuestión.

Ingeniero de redes

Los ingenieros están más compenetrados con los bits y bytes de una red. Es típico que tengan un grado académico en ingeniería eléctrica y se espera que sean expertos en los sistemas operativos de red con los que trabajan y, en especial, en elementos clave del hardware de la red, como sus concentradores, ruteadores, switches, etc. También son considerados como el personal que, como último recurso, repara la red y diagnostica y soluciona los problemas más enfadosos que superan la capacidad del administrador de la red.

Aparte de tener un grado académico, los ingenieros de red poseen, generalmente, al menos cinco años de experiencia en operación y reparación de redes complejas. Asimismo, tienen certificaciones de las compañías que fabrican equipo de conectividad de redes, como el reconocido programa de certificación de Cisco.

Arquitecto/diseñador de red

Los arquitectos de red (a menudo llamados diseñadores de red) trabajan, en general, para compañías que venden y dan soporte a redes o para grandes empresas que tienen redes enormes que están en constante cambio y expansión. En esencia, los arquitectos de red diseñan redes y necesitan combinar cualidades importantes para ser exitosos. Deben comprender las necesidades del negocio que la red necesita satisfacer, así como conocer a fondo todos los productos de conectividad de redes disponibles en el mercado y la forma en que éstos interactúan. Los arquitectos de red también son importantes cuando se necesita expandir una red compleja y ayudan a asegurar que las nuevas adiciones no provoquen problemas.

Otros puestos de trabajo relacionados con las redes

Existe una amplia variedad de puestos de trabajo relacionados con las redes, entre ellos algunos que no están vinculados directamente con la red, como el administrador de la base de datos. Otros incluyen al administrador de correo electrónico, al webmaster, al diseñador de web, al técnico de soporte de red y otros. En realidad, una lista interminable de puestos de trabajo diferentes se encuentran disponibles en el campo de la conectividad de redes.

Si está decidido a entrar en el campo de la conectividad de redes, es aconsejable que invirtiera tiempo en consultar los anuncios donde solicitan diferentes trabajos en conectividad y ver qué requisitos son necesarios para cubrir esos puestos. Una vez que haya encontrado el trabajo que refleje sus intereses, podrá analizar las habilidades adicionales que se requieren así como los cursos o las certificaciones que fueran necesarias para acceder a ese trabajo. Existen muchas oportunidades. Lo importante es comenzar y cumplir sus objetivos.

LEY SARBANES-OXLEY DE 2002

Probablemente se estará preguntando qué tiene que ver una ley que sancionó el Congreso de Estados Unidos con el campo de la conectividad de redes y por qué se incluye en este libro. La razón es que esta ley tiene un efecto significativo en las redes de todas las compañías públicas,

por lo que es importante que usted comprenda de qué se trata. Por cierto, mientras que esta ley fue sancionada en el año 2002, algunas de sus partes se implantaron en tiempos diferentes, con algunas de sus fechas límite extendiéndose hasta el año 2007 aproximadamente.

La ley Sarbanes-Oxley de 2002 (conocida como SOX, se pronuncia "socks") fue una acta patrocinada por el Senador Sarbanes y el Representante Oxley en respuesta de los múltiples casos de malas prácticas corporativas que le precedieron, como Enron, Global Crossing, Arthur Andersen, Tyco y otras. La ley introduce cambios significativos en gran número de áreas de la administración y la contabilidad corporativas. Es probable que un cambio en particular afecte a la mayoría de los profesionales de la conectividad, en particular, a los involucrados en las operaciones diarias de las redes, como los administradores de red.

La sección 404 de la ley impone a las compañías públicas nuevas obligaciones, entre ellas, evaluar anualmente su sistema de controles internos. Además, sus auditores externos deben examinar dichos controles y dar fe de la eficiencia de ellos para el reporte correcto de la información financiera de la compañía. Podría parecer que estas exigencias sólo involucrarían a los departamentos de contabilidad de las empresas y, en realidad, en su mayoría es así. Sin embargo, los controles internos de la contabilidad dependen en gran medida de los controles del sistema de red, en particular de los que afectan los sistemas importantes que utiliza la compañía para la administración y el reporte de información financiera. Usted seguramente debe saber que muchas partes de SOX representan en la actualidad obligaciones para las principales bolsas de valores, como NYSE y NASDAQ, por lo que el cumplimiento de dicha ley es de gran importancia para todas las compañías públicas.

En general, los auditores externos clasifican a los sistemas de las compañías como dentro del alcance de su auditoría ("in scope") o fuera del alcance de su auditoría. Los sistemas "in scope" incluyen el de contabilidad de la compañía, el de nómina, los sistemas de administración de acciones, los de administración de materiales, los de embarque, los de cobranza, los sistemas financieros y otros por el estilo. Las computadoras y todo el hardware y el software que realizan esas funciones o que almacenan y operan el software que lleva a cabo esas funciones son también "in scope". Otras operaciones de red que soportan esos sistemas pueden ser también "in scope", como el establecimiento de las contraseñas de toda la red, los procedimientos de respaldo y el establecimiento de la administración de las cuentas de usuario nuevas y eliminadas, etcétera.

De acuerdo con lo anterior, los administradores de red de las compañías públicas que cotizan en la bolsa necesitarán trabajar muy de cerca con sus departamentos de contabilidad a fin de cumplir con los requerimientos de SOX 404 a medida que cambien las circunstancias. Lo anterior implica llevar a cabo actividades como las siguientes:

- Documentar todas las actividades concernientes a la creación, el mantenimiento y la desactivación de las cuentas de usuario, incluyendo el acceso apropiado de usuarios nuevos, modificados y cancelados en los sistemas "in scope".
- Crear un control de cambios para cualquier sistema que la compañía modifique ocasionalmente, como un sistema de contabilidad para el que utilice reportes desarrollados por encargo o programas de procesamiento.
- Documentar los parámetros de seguridad de la red.
- Documentar los parámetros de seguridad, las actividades de mantenimiento y la administración de cuentas de usuario y contraseñas de los sistemas "in-scope".
- Documentar las actividades rutinarias de mantenimiento de los sistemas "in-scope".

- Trabajar con el grupo de contabilidad y con los auditores para demostrar que todos los controles que se han adoptado se han aplicado sin excepciones.
- Crear y mantener sistemas (incluyendo los de procedimientos manuales) a fin de detectar cambios no autorizados.

Obviamente, un libro acerca de la conectividad de redes no puede abordar en su totalidad todos los factores que involucra el cumplimiento de la ley Sarbanes-Oxley. Sin embargo, es aconsejable que tenga una idea general de qué es y qué involucra. Los profesionales en contabilidad encargados de cumplir este requerimiento contarán con información más detallada acerca de qué pasos se requieren exactamente para su compañía.

RESUMEN DEL CAPÍTULO

Mucha gente que he conocido que trabaja en algún área de la tecnología de la información, como la conectividad de redes, no considera las razones desde el punto de vista del negocio de las redes cuando asisten cotidianamente a sus trabajos o proponen mejoras a la red. Ciertamente, esta actitud no se limita al campo de la conectividad; muchas personas que trabajan en algún área de la compañía a veces pasan por alto que la razón por la que su función existe es proporcionar soporte a los objetivos. Los empleados más exitosos de cualquier compañía están convencidos firmemente de por qué hacen lo que hacen, antes de considerar cómo hacerlo mejor. Algunas sugerencias de este capítulo le ayudarán a dominar la administración y mejorar una red de manera exitosa, sin olvidar los beneficios que la red brinda a la compañía. Una vez que conoce lo que necesita la compañía, puede proponer las mejores soluciones para resolver los problemas que se pudieran presentar o realizar las mejoras adecuadas a la red.

En este capítulo también se analizaron algunas áreas significativas en las que usted puede adentrarse en la tecnología de la conectividad de redes si se decide. La demanda de personal calificado es extremadamente alta y los sueldos muy atractivos. Además, las personas que trabajan en este campo tienen empleos que son, en su mayoría, divertidos, estimulantes y gratificantes en muchas formas.

Por último, usted aprendió un poco acerca de la ley Sarbanes-Oxley de 2002 y su efecto en los profesionales que se dedican a la conectividad de redes.

El capítulo siguiente comienza con la exploración de los detalles técnicos de la conectividad de redes mediante un breve análisis de algunos conceptos básicos sobre la ciencia de la computación que es necesario que conozca. Si ya tiene conocimientos acerca de los diferentes sistemas numéricos y de cómo se miden las velocidades de transmisión de datos, es probable que desee saltar el capítulo siguiente e ir directamente a los temas sobre conectividad de redes que siguen, pero le debo advertir que es necesario que tenga una muy buena idea de cómo funcionan los números binarios a fin de comprender algunos análisis que se llevan a cabo en el capítulo 8 acerca de los protocolos de red.



CAPÍTULO 2

Presentación de las bases

Usted no necesita un doctorado en ciencias de la computación para convertirse en una persona eficiente en el campo de la conectividad de redes, pero sí necesita comprender algunos de los fundamentos de la materia. En este capítulo se analizan la terminología y los conocimientos básicos que debe tener a fin de que la información contenida en lo que resta del libro le sea más comprensible y de mayor utilidad.

Si ha trabajado con las computadoras por algún tiempo y, especialmente, si se ha capacitado o tiene experiencia como programador de computadoras, no es necesario que lea detalladamente este capítulo. Sin embargo, es recomendable que lo repase para que se sienta completamente seguro de que ya domina el tema a fondo.

BITS, NIBBLES Y BYTES

La mayoría de las personas saben que las computadoras, en su nivel más elemental, trabajan sólo con 1 y 0. A cada uno de estos números (ya sea 0 ó 1) se le llama bit, que es una abreviatura de *dígito binario*. Coloque juntos ocho bits y tendrá un *byte*; coloque juntos 1 000 bits y tendrá un *kilobit*, o coloque 1 000 bytes y tendrá un *kilobyte*. (Una unidad que se utiliza muy de vez en cuando se compone de una serie de cuatro bits y se llama *nibble*. Recuerde esto para cuando juegue *Jeopardy*!).

Comprensión de los números binarios

Antes de que aprenda acerca de los números binarios, es de utilidad recordar algunas cosas sobre el sistema de numeración que la gente utiliza cotidianamente, llamado *sistema de numeración decimal* o *sistema de numeración base 10*. El sistema de numeración decimal está construido mediante el empleo de diez símbolos diferentes, cada uno de los cuales representa una cantidad del cero al nueve. Por tanto, se pueden utilizar 10 dígitos posibles, del 0 al 9. (El sistema de numeración base 10 toma su nombre del hecho de que sólo es posible que el sistema tenga diez dígitos).

Una parte fundamental de cualquier sistema de numeración es el uso de *posiciones* en las que pueden colocarse los símbolos numéricos. Cada posición asigna un valor diferente al número que se representa. Por tanto, en el sistema decimal el número 10 representa la cantidad diez. Hay un 1 en la *posición de las decenas* y un 0 en la *posición de las unidades*. Lo anterior también puede representarse como $(1 \times 10) + (0 \times 1)$. Con base en este mismo razonamiento, considere el número 541. Este número utiliza la posición de las centenas así como también las posiciones de las decenas y unidades. Puede representarse como $(5 \times 100) + (4 \times 10) + (1 \times 1)$, o puede decir este número como quinientos más cuarenta más uno.

Cada número escrito tiene un *dígito menos significativo* y un *dígito más significativo*. El primero es el que se encuentra más hacia la derecha, mientras que el segundo es el que se encuentra más hacia la izquierda. En el caso de los números binarios, también se habla sobre los bits más o menos significativos, pero el significado es el mismo.

Hasta el momento, esta sección ha servido simplemente para repasar el conocimiento básico de los números que aprendió en la escuela. Lo que no aprendió ahí es el hecho de que es completamente arbitrario basar un sistema de numeración en el diez; no existe ninguna razón matemática en favor de un sistema base 10 sobre cualquier otro. Usted puede inventar siste-

mas de numeración en cualquier base que desee. Puede tener una sistema de numeración base 3, un sistema de numeración base 11 o cualquier otro que desee o necesite. Los seres humanos han tenido preferencia por el sistema base 10 probablemente porque tenemos diez dedos y, por tanto, tendemos a pensar en decenas. Las computadoras, por otro lado, tienen sólo dos dígitos con qué trabajar, 1 y 0, por lo que necesitan utilizar un sistema de numeración diferente. El sistema de numeración natural que utiliza una computadora es base 2. A este sistema también se le conoce con el nombre de *sistema de numeración binario*. Las computadoras utilizan solamente 1 y 0 en su nivel más básico debido a que sólo entienden dos estados: encendido y apagado. En el sistema de numeración binario, un 1 representa encendido, mientras que un 0 representa apagado.

Recuerde que en el sistema de numeración decimal, la posición de cada número es importante. Lo mismo sucede en el binario, sólo que cada posición no corresponde a potencias de 10, sino a potencias de 2. A continuación se presentan los valores de las ocho posiciones menos significativas que se utilizan en el sistema de numeración binario:

128	64	32	16	8	4	2	1

Por tanto, suponga que tiene el número binario siguiente:

1	0	1	0	1	1	0	1

Debe seguir los mismos pasos que utilizaría para comprender un número en el sistema de numeración decimal: en este ejemplo, el número binario representa 128 + 32 + 8 + 4 + 1, esto es, 173 en el sistema decimal. Usted también puede escribir (o calcular) este número como sigue:

$$(128 \times 1) + (64 \times 0) + (31 \times 1) + (16 \times 0) + (8 \times 1) + (4 \times 1) + (2 \times 0) + (1 \times 1)$$

De forma que son básicamente dos cosas las que diferencian el sistema de numeración decimal del binario: el sistema binario utiliza solamente 1 y 0 para representar cualquier valor, a la vez que el valor de los números en las diferentes posiciones varía.

Usted se preguntará cómo se puede determinar si usted está leyendo un número binario o uno decimal. Por ejemplo, si está leyendo un libro acerca de computadoras y ve el número 10101, ¿cómo sabe si dicho número representa el diez mil ciento uno o el veintiuno? Existen algunas cosas diferentes que se pueden decir. Primero, en general los números binarios se muestran con al menos ocho posiciones (un byte completo), aun si los dígitos del principio del número son 0. Segundo, si usted ve una serie de números que son 1 y 0 solamente, es muy probable que esté frente a números binarios. Tercero, los números binarios no utilizan el punto decimal para representar valores fraccionarios; el número 10 100.01 se supone que es un número del sistema decimal. Cuarto, los números decimales deben utilizar comas, como aprendió en la escuela. Por ello, el número 10 100 debe leerse como diez mil cien, mientras que el número 10100 debe leerse como el número binario de la cantidad veinte. Quinto, a veces la gente escribe la letra *b* al final de un número binario, aunque esta convención no se utiliza ampliamente. Tome en cuenta todas estas cosas más un poco de sentido común y, seguramente, no tendrá dudas para saber si está frente a un número binario o uno decimal.

¿Cómo convertir rápidamente números hexadecimales, decimales, octales y binarios?

La calculadora que viene con todas las versiones de Windows le permite convertir valores de una manera rápida en hexadecimal, decimal, octal y binario. Con la calculadora abierta, póngala en modo Científico (abra el menú View y seleccione Scientific). Este modo muestra en la calculadora muchas características avanzadas. En el área de la esquina superior izquierda de la calculadora puede observar cuatro botones de opciones con la leyenda Hex, Dec, Oct y Bin, los cuales corresponden a los sistemas de numeración hexadecimal, decimal, octal y binario, respectivamente. Seleccione qué sistema desea utilizar para ingresar un número y después teclee sobre cualquiera de las otras opciones para convertir el número de manera instantánea. Por ejemplo, suponga que teclea el botón de la opción Bin e ingresa el número 110100100110111010l. Si usted teclea después el botón Dec, la calculadora despliega que el número que acaba de ingresar es el 215 482 en el sistema decimal. O, si teclea el botón Hex, encontrará que el número binario que usted ingresó es el 349BA en el sistema de numeración hexadecimal. De la misma manera, si teclea el botón Oct, observará que el número es 644672 en el sistema de numeración octal. También puede desplazarse en la otra dirección: seleccione el botón Dec, ingrese algún número y después teclee los botones opcionales para ver la equivalencia en otros sistemas de numeración. (Aprenderá más acerca de los sistemas de numeración octal y hexadecimal en la sección siguiente).

Otros sistemas de numeración importantes

Existen otros dos sistemas de numeración importantes que encontrará en el mundo de la conectividad de redes: el octal y el hexadecimal. El hexadecimal se utiliza más que el octal, pero es aconsejable que aprenda ambos.

El sistema de numeración octal también se conoce con el nombre de sistema de numeración base 8. En este esquema, la posición de cada número sólo puede tener dos valores: 0 y 7. El número 010 en el sistema de numeración octal corresponde al 8 en el sistema de numeración decimal. Los números en octal pueden indicarse con un cero o un signo de por ciento (%) al principio, o con una letra O en mayúsculas al final.

El sistema de numeración hexadecimal es muy común en el campo de la conectividad de redes y, a menudo, se utiliza para representar direcciones de red, direcciones de memoria y cosas por el estilo. El sistema hexadecimal (también llamado sistema de numeración base 16) puede utilizar 15 números diferentes en cada posición. Puesto que solamente hemos escrito números del 0 al 9, el sistema hexadecimal utiliza de la letra *A* a la *F* para representar los símbolos extra.

Los números hexadecimales están precedidos, por lo general, por un cero seguido de una letra *x* y, después, el número hexadecimal. La letra *x* puede estar en mayúsculas o en minúsculas, por lo que 0 x 11AB y 0 X 11AB son igualmente válidos. Los números hexadecimales también pueden mostrarse con una letra *h* al final, la cual puede estar en minúsculas o en ma-

yúsculas. Es raro que estén precedidos por el signo de pesos ($) (por ejemplo, $11AB). A menudo, podrá reconocer fácilmente los números hexadecimales simplemente por el hecho de que, en general, los valores incluyen algunas letras (de la *A* a la *F*). En los números hexadecimales, la *A* equivale al 10 del sistema decimal, la *B* equivale al 11, la *C* al 12, la *D* al 13, la *E* al 14 y la *F* al 15.

Puede determinar el valor decimal de un número hexadecimal de forma manual utilizando el mismo método que se mostró para el caso de los números decimales y binarios. Los valores de las posiciones de los cuatro primeros dígitos son

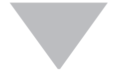
4096	256	16	1

Por tanto, el número 0 × 11AB puede convertirse a decimal con la fórmula (1 × 4096) + (1 × 256) + (10 × 16) + (11 × 1), o 4 523 en decimal.

TERMINOLOGÍA BÁSICA PARA DESCRIBIR LAS VELOCIDADES EN LA CONECTIVIDAD DE REDES

El negocio de la conectividad de redes trata, casi en su totalidad, acerca de la transferencia de datos de un punto a otro. Por esta razón, uno de los aspectos más importantes que es necesario que comprenda acerca de cualquier conexión de red es la cantidad de datos que ésta puede transmitir. En general, a esta capacidad se le conoce con el nombre de *ancho de banda*, la cual se mide por la cantidad de datos que puede transferir una conexión en un determinado periodo.

La unidad de medida más común del ancho de banda es *bits por segundo*, abreviada como bps. El ancho de banda es, en términos simples, el número de bits que una conexión puede transferir en un segundo. Es muy común utilizar los diferentes múltiplos de esta medida, dentro de los que se incluyen miles de bits por segundo (Kbps), millones de bits por segundo (Mbps) o miles de millones de bits por segundo (Gbps).



PISTA Recuerde que bits por segundo no es igual a bytes por segundo. Para convertir a bytes por segundo cuando se conocen los bits por segundo (aproximadamente), divida el número de bps entre 8. En este libro, para expresar bits por segundos, siempre se utiliza una letra minúscula b, mientras que para expresar bytes por segundo siempre se utiliza una letra mayúscula B (por ejemplo, 56 Kbps es 56 mil bits por segundo, mientras que 56 kBps es 56 mil bytes por segundo).

Una medida estrechamente relacionada es el Hertz, que es el número de ciclos que se transfieren por segundo. El Hertz se abrevia *Hz* y se pronuncia "hurts". De la misma forma que los *bps*, se escucha más sobre los múltiplos del Hertz, incluyendo miles de Hertz (KHz o kilohertz) y millones de Hertz (MHz o megahertz). Un microprocesador que opera a 100 MHz, por ejemplo, trabaja a 100 millones de ciclos por segundo. En Estados Unidos, la electricidad trabaja a 60 Hz; en Europa a 50 Hz. Los Hertz y los bits por segundo, en esencia, son lo mismo y a menudo se usan de forma intercambiable. Por ejemplo, se dice que Ethernet opera a 10 MHz y también transporta 10 Mbps de información.

RESUMEN DEL CAPÍTULO

Mientras que éste es un libro sobre conectividad de redes para principiantes, hubiera tenido que ser del doble de tamaño si tuviera que explicar cada término de la conectividad de redes cada vez que se utilizan. En lugar de eso, en el resto del libro usted conoce los conceptos básicos que se presentan en este capítulo, así como la información que se encuentra en el glosario en la parte final. La mayoría de las personas no lee los glosarios hasta que se topa con un término que desconoce. Yo recomendaría que, en lugar de hacer lo anterior, invierta algunos minutos en la revisión del glosario antes de leer los capítulos siguientes, a fin de asegurarse de conocer cualquier término que se utilice. Los términos *nodo*, *anfitrión*, *ancho de banda*, *banda base*, *estación de trabajo*, *cliente* y *servidor* son algunos ejemplos de términos con los que debería estar familiarizado y que se supone que conoce. El glosario incluye estos términos y muchos más.

En el capítulo siguiente aprenderá acerca de los tipos básicos de red y sobre un modelo conceptual importante de conectividad de redes que encontrará muy a menudo cuando trabaje con redes: el modelo de Interconexión de sistemas abiertos (OSI). El modelo OSI se utiliza virtualmente en cada aspecto de la conectividad de redes y proporciona un marco de referencia sobre cómo funcionan las redes.

CAPÍTULO 3

La conectividad de redes

La conectividad de redes puede ser un tema muy complejo, pero usted encontrará que puede ser un profesional extremadamente eficiente en este campo sin tener que estudiar un doctorado en ciencias de la computación. Sin embargo, existen *muchos* aspectos de la conectividad de redes, lo que tiende a hacer que el tema parezca mucho más complejo de lo que es en realidad. En este capítulo aprenderá acerca de los aspectos fundamentales de la conectividad de redes, con lo cual tendrá los elementos necesarios para comprender con más detalle los temas posteriores. Asimismo, se estudian algunos términos básicos clave acerca de la conectividad de redes y se proporciona un panorama de la información detallada sobre el tema.

Si es principiante en la tecnología de la conectividad de redes, adquirir un buen conocimiento de los fundamentos que se presentan en este capítulo le permitirá construir una marco conceptual con el cual pueda manejar los conocimientos más detallados, tal como se presentan más adelante en el libro. Además, el resto del libro supone que usted está familiarizado con todos los conceptos que se presentan en este capítulo.

CONOCIENDO LOS TIPOS DE RELACIONES ENTRE LAS REDES

El término *relaciones entre redes* se refiere a dos conceptos diferentes acerca de la forma en que una computadora utiliza los recursos de otra a través de la red.

Existen dos tipos de relaciones fundamentales entre redes: de igual a igual y cliente/servidor, (de hecho, uno puede referirse a ellas como *filosofías de red*) y definen la estructura básica de una red. Para comprenderlas mejor, se pueden comparar con las diferentes filosofías de la administración de negocios. Una *red de igual a igual* se parece mucho a una compañía que opera mediante una filosofía de administración descentralizada, donde las decisiones se toman localmente y los recursos se administran de acuerdo con las necesidades más inmediatas. Una red *cliente/servidor* se asemeja a una compañía que se basa en una administración centralizada, donde las decisiones son tomadas en un punto central por un grupo relativamente pequeño de personas. A menudo se presentan circunstancias donde ambos esquemas son adecuados y muchas redes muestran aspectos de ambos tipos.

Tanto las redes de igual a igual como las de cliente/servidor deben tener ciertas capas de red en común. Ambos tipos requieren una conexión física a la red entre las computadoras, que se utilicen los mismos protocolos de red, etc. En este sentido, no existen diferencias entre los dos tipos de relaciones de red. La diferencia estriba en si se distribuyen entre todas las computadoras los recursos compartidos de la red o si se utilizan servidores de red centralizados.

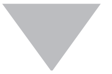


NOTA La mecánica de funcionamiento real de una red puede dividirse en capas. El concepto de capas y los que hay en cada una de ellas se describirá con más detalle en este capítulo.

Relaciones en una red de igual a igual

Una *relación en una red de igual a igual* se define como una donde las computadoras de la red se comunican entre sí al mismo nivel. Cada computadora es responsable de poner a disposición de los otros ordenadores de la red sus propios recursos, los cuales pueden ser archivos, directorios,

programas de aplicación o dispositivos, como impresoras, módems o tarjetas de fax, o cualquier otra combinación. Cada computadora es también responsable de configurar y mantener la seguridad de estos recursos. Por último, cada computadora es responsable de acceder a los recursos de red que ésta necesite de otras computadoras de igual a igual y de saber dónde se encuentran dichos recursos y qué seguridad se requiere para acceder a los mismos. La figura 3-1 muestra cómo esto funciona.



NOTA Incluso en una red de igual a igual, es posible utilizar una computadora dedicada a acceder con cierta frecuencia a los recursos de la red. Por ejemplo, puede asignar la aplicación y los archivos de datos de un sistema de contabilidad a una sola estación de trabajo y no utilizar esa computadora para realizar las tareas típicas de una estación, como el procesamiento de palabra, de forma que toda la capacidad de la computadora esté disponible para el sistema de contabilidad. La computadora se encontraría trabajando como una red de igual a igual, sólo que no se utilizaría para otro propósito.

Relaciones de red cliente/servidor

Una *relación de red cliente/servidor* es en la que se distingue entre las computadoras que ponen a disposición los recursos de la red (los *servidores*) y aquéllas que utilizan los recursos (los *clientes* o las *estaciones de trabajo*). Una red cliente/servidor pura es una en la que todos los recursos de red disponibles —como archivos, directorios, aplicaciones y dispositivos compartidos— residen y están administrados centralmente y, después, son accesados por las computadoras cliente. Ninguna de éstas comparte sus recursos con otras computadoras cliente o con los servidores. En lugar de eso, las computadoras cliente son exclusivamente consumidoras de estos recursos.

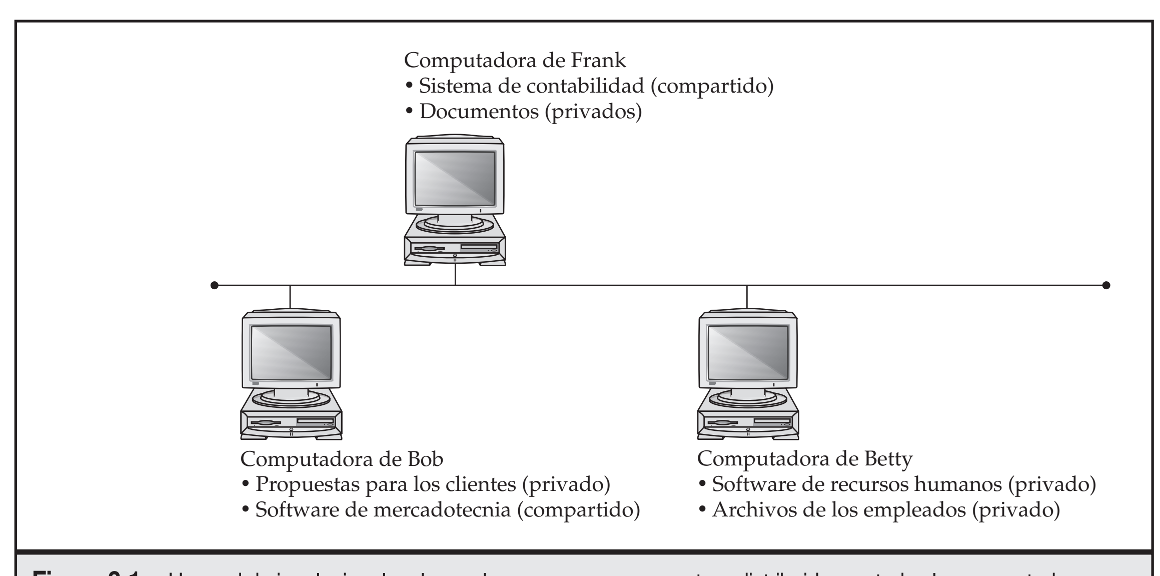


Figura 3-1. Una red de igual a igual en la que los recursos se encuentran distribuidos en todas las computadoras.



NOTA No confunda las redes cliente/servidor con los sistemas de base de datos cliente/servidor. Mientras que ambos significan los mismos (conceptualmente), una base de datos cliente/servidor es una donde el procesamiento de aplicación se divide entre el servidor de la base de datos y los clientes de la misma. El servidor es responsable de responder las solicitudes de datos de los clientes, así como de proporcionarles los datos adecuados, mientras que los clientes son responsables de formatear, desplegar e imprimir esos datos para el usuario. Por ejemplo, Novell NetWare o Windows 2000 Server son sistemas operativos de red cliente/servidor, mientras que la base de datos Oracle o la SQL Server, de Microsoft, son sistemas de base de datos cliente/servidor.

Las computadoras servidoras instaladas en una red cliente/servidor son responsables de poner a disposición y administrar los recursos compartidos apropiados, así como de administrar la seguridad de los mismos. La figura 3-2 muestra dónde estarían ubicados los recursos en esa red.

Comparación de las redes de igual a igual y las cliente/servidor

Como se mencionó, la mayoría de las redes tienen características tanto de relaciones de igual a igual como de cliente/servidor. Mientras que es ciertamente posible —y a veces deseable— tener sólo un tipo de relación, el hecho es que ambas tienen su aplicación. Antes de tomar la decisión de configurar una red con base en uno o ambos tipos de relaciones, usted tiene que analizar las ventajas y desventajas de cada una y determinar cómo cumplen sus necesidades y las de su compañía. Considere las ventajas y desventajas de usar una red de igual a igual que se enuncian a continuación.

Figura 3-2. Una red cliente/servidor mantiene los recursos centralizados.

Ventajas de las redes de igual a igual

Existen varias ventajas en el uso de las redes igual a igual, en particular en compañías pequeñas, como las siguientes:

- **Utilizan hardware de cómputo más barato** Las redes de igual a igual trabajan con una carga de trabajo baja. Esto significa que los recursos se encuentran distribuidos en muchas computadoras, de forma que no existe la necesidad de una computadora que actúe como servidor. El efecto en cada estación de trabajo es, en general (sin embargo, no siempre), relativamente menor.
- **Fácil de administrar** Estas redes son, ante todo, más fáciles de configurar y administrar. Debido a que cada máquina lleva a cabo su propia administración —generalmente sobre ciertos recursos limitados— el esfuerzo que se requiere para administrar la red se distribuye entre mucha gente.
- **No se requiere de un NOS** Las redes igual a igual no requieren de un sistema operativo de red (NOS). Usted puede construir una red de este tipo utilizando solo Windows 98, Windows 2000 o Windows XP en todas las estaciones de trabajo o en todas las computadoras Macintosh para ese propósito. Todos estos sistemas operativos del cliente incluyen todas las características necesarias para hacerlo. De manera similar, también puede hacerlo con todas las computadoras que tengan instalado UNIX o LINUX (aunque esto es en realidad más difícil de configurar y dar mantenimiento, por el hecho de que UNIX y LINUX son muy poderosos y complejos).
- **Más redundancia integrada** Si tiene una computadora pequeña, de 10 a 20 estaciones de trabajo con información importante en cada una, y cualquiera de ellas falla, aún tiene disponibles la mayor parte de los recursos. Una red igual a igual puede ofrecer más redundancia que una red cliente/servidor ya que un número menor de puntos de falla pueden afectar a toda la red y a cada usuario.

Desventajas de las redes igual a igual

Existen también varias desventajas en las redes igual a igual, en particular, en redes de gran tamaño o en aquellas que tienen requerimientos más complejos o perfeccionados, como los siguientes:

- **Puede afectar el desempeño del usuario** Si algunas estaciones de trabajo han utilizado recursos instalados en ellas, el uso de dichos recursos por parte de los demás usuarios conectados a la red puede afectar adversamente a la persona que esté utilizando la estación de trabajo donde están instalados los recursos.
- **No son muy seguras** Las redes igual a igual no son tan seguras como las redes cliente/servidor, ya que no se puede garantizar —sin importar qué tan buenos sean los usuarios de la red— que quienes la utilicen administren de manera adecuada sus máquinas. En realidad, en una red de cualquier tamaño (digamos, de más de diez usuarios), usted puede estar casi seguro de que al menos algunos de ellos no sigan las buenas prácticas de administración en sus propias máquinas. Sin embargo, los sistemas operativos de escritorio más comunes con los que se opera una red de este tipo, como Windows XP o Macintosh, no están diseñados para ser sistemas operativos de red seguros.

- **Difíciles de respaldar** El respaldo confiable de todos los datos distribuidos en varias estaciones de trabajo es difícil, y no es recomendable asignar este trabajo al usuario de cada máquina. La experiencia ha mostrado que dejar esta vital tarea a los usuarios significa que no se va a llevar a cabo.
- **Difícil de mantener un control de las versiones** En una red de este tipo, con archivos almacenados potencialmente en diferentes máquinas, puede ser extremadamente difícil controlar las versiones de los diferentes documentos.

Ventajas de las redes cliente/servidor

Las redes cliente/servidor, por otra parte, ofrecen la oportunidad de tener una administración centralizada y utilizan equipo que es más apropiado para administrar y proporcionar cada recurso. Además, son el tipo de red que usted casi siempre puede observar en sitios con más de diez usuarios, y existen muchas buenas razones para ello, como las que se enuncian a continuación:

- **Son muy seguras** La seguridad de una red cliente/servidor depende de muchos aspectos. En primer lugar, debido a que los recursos compartidos se encuentran ubicados en un área centralizada, pueden administrarse en ese punto. La administración de un gran número de recursos es mucho más fácil si se encuentran en uno o dos servidores, a diferencia de administrar los recursos de diez o cien computadoras. En segundo lugar, generalmente los servidores están ubicados físicamente en un lugar seguro, como un centro de cómputo cerrado con llave. La seguridad física es un aspecto importante de las redes y no puede lograrse en una red igual a igual. En tercer lugar, los sistemas operativos sobre los que opera una red cliente/servidor están diseñados para ser seguros. Siempre y cuando se lleven a cabo buenas prácticas de seguridad y administración, los servidores no podrán ser accesados fácilmente sin permiso.
- **Mejor desempeño** Mientras que los servidores dedicados son más costosos que las estaciones de trabajo estándar, los primeros ofrecen un desempeño considerablemente mejor y están diseñados para manejar las necesidades de múltiples usuarios de forma simultánea.
- **Respaldo centralizado** Respaldar la información crítica de una compañía es mucho más fácil cuando ésta se encuentra centralizada en un servidor. A menudo, dichas tareas de respaldo pueden llevarse a cabo en la noche cuando el servidor no se utiliza y los datos están estáticos. Aparte de ser más fácil, los respaldos centralizados son también mucho más rápidos que los respaldos descentralizados.
- **Muy confiables** A pesar de que es verdad que existe más redundancia implícita en una red de igual a igual, también es cierto que una buena red cliente/servidor, en conjunto, puede ser más confiable. Con frecuencia los servidores dedicados tienen mucha más redundancia implícita que las estaciones de trabajo estándar. Éstas pueden manejar la falla de un controlador de disco, de una fuente de alimentación o un procesador y continuar trabajando hasta que el componente que falla sea reemplazado. Asimismo, debido a que un servidor dedicado tiene que llevar a cabo sólo una tarea relativamente simple, su complejidad se reduce y su confiabilidad aumenta. Compare este panorama con una red de igual a igual, donde las acciones por parte de los usuarios puede reducir

de manera drástica la confiabilidad de cada una de las estaciones de trabajo. Por ejemplo, tener que reiniciar una PC o una Macintosh con mucha frecuencia es muy común, mientras que los servidores dedicados a menudo trabajan por meses sin requerir que se reinicien o que se pierda la información.

Desventajas de las redes cliente/servidor

Haciendo un balance de las ventajas de las redes cliente/servidor, es necesario que se de cuenta que existen desventajas, en particular para las compañías que no poseen su propia administración de red dentro de ellas, o que quieren minimizar el costo de la red lo más posible:

- **Requieren de administración profesional** Las redes cliente/servidor necesitan, en general, algún nivel de administración profesional, incluso las más pequeñas. Usted puede contratar un administrador de red o recurrir a una compañía que ofrezca servicios profesionales, pero es importante recordar que en general se requiere de una administración profesional. El conocimiento de todos los detalles de un sistema operativo de red es importante y requiere de experiencia y capacitación.
- **Uso más intenso del hardware** Además de las computadoras del cliente, también necesita un servidor que, en general, debe ser un equipo muy "poderoso", con mucha memoria y espacio en disco. Además, necesita un sistema operativo de red y un número de licencias de cliente adecuado, lo cual agrega al menos varios miles de dólares al costo del servidor. En computadoras grandes, se incrementa el costo a varias decenas de miles de dólares.

En pocas palabras, seleccione una red de igual a igual para redes pequeñas con un número de usuarios menor a 10 ó 15, y opte por una red cliente/servidor cuando la red sea mayor. Debido a que la mayoría de las redes se encuentran instaladas bajo un concepto cliente/servidor, en la mayor parte de este libro se supone este tipo de red.

CARACTERÍSTICAS DE LAS REDES

Ahora que ya conoce las dos formas básicas en las que las computadoras en una red pueden interactuar entre sí, es importante que conozca los tipos de cosas que puede hacer con una red. En las secciones siguientes se estudian las características y capacidades más comunes de las redes.

Compartición de archivos

Originalmente, la *compartición de archivos* fue la razón primordial para tener una red. En realidad, las compañías de pequeño y mediano tamaños, a mediados de los ochenta, por lo regular instalaban redes con el objeto de llevar a cabo esta tarea. A menudo, las características de la instalación las dictaba la necesidad de automatizar los sistemas de contabilidad. Por supuesto, una vez que las redes se encontraban instaladas, se hizo más fácil la compartición de otros tipos de archivos, como de procesamiento de palabra, hojas de cálculo y otros a los que mucha gente necesitaba acceder en forma regular.

La *compartición de archivos* requiere un directorio compartido o controlador de disco que pueda ser accesado por muchos usuarios de la red, junto con la lógica de programación asociada que se necesita para asegurarse de que más de una persona no realice cambios conflictivos a un

archivo al mismo tiempo (llamado *bloqueo de archivos*). La razón por la que usted no desearía que más de una persona realice cambios en un archivo al mismo tiempo es que ninguno de ustedes se percataría del problema. La mayoría de los programas de software no posee la característica de permitir cambios múltiples a un solo archivo al mismo tiempo y de resolver los problemas que puedan presentarse. (La excepción a esta regla es que la mayoría de los programas de base de datos permite que múltiples usuarios accedan a la base de forma simultánea pero, aun en ese caso, lo hacen mediante una técnica llamada *bloqueo de renglón*, la cual restringe la realización de cambios en un determinado campo a un solo usuario al mismo tiempo).

De forma adicional, los sistemas operativos de red que llevan a cabo la compartición de archivos también administran la seguridad de esos archivos compartidos. Esta seguridad puede controlar, con un gran nivel de detalle, quién tiene acceso a qué archivos y qué tipos de acceso tienen. Por ejemplo, algunos usuarios pueden tener permiso de ver sólo ciertos archivos compartidos, mientras que otros tienen permiso para editar o incluso eliminar algunos de ellos.

Compartición de impresoras

Un competidor muy cercano en importancia a la compartición de archivos es la *compartición de impresoras*. Mientras que es verdad que las impresoras láser son, en la actualidad, tan baratas que se pueden instalar en cada oficina si así se desea, la compartición de ellas entre los usuarios de la red es, en general, aún más económica. Ésta le permite reducir el número de impresoras que necesita y también le permite ofrecer impresoras de mayor calidad. Por ejemplo, una impresora láser a color cuesta aproximadamente $5 000. Las copiadoras digitales más novedosas que pueden manejar trabajos de impresión más voluminosos a más de 60 páginas por minuto pueden tener un costo de más de $30 000. Como puede ver, la compartición de dichas impresoras entre muchos usuarios tiene sentido.

Ésta puede llevarse a cabo de muchas maneras en una red. La más común es utilizar *colas de impresión* en un servidor. Una cola de impresión maneja trabajos de impresión hasta que se terminen de llevar a cabo y después, de forma automática, envía los trabajos en espera a la impresora. El uso de una cola de impresión es eficiente en las estaciones de trabajo, ya que pueden enviar a imprimir rápidamente sin tener que esperar a que la impresora procese cualquier trabajo en espera. Otra forma de compartir impresoras en una red es permitir que cada estación de trabajo acceda a la impresora directamente (la mayoría de las impresoras puede configurarse de forma que se puedan conectar a la red de la misma manera que una estación de trabajo) pero, generalmente, cada una deberá esperar su turno si muchas estaciones de trabajo quieren usar la impresora al mismo tiempo.

Las impresoras de red que utilizan colas de impresión siempre cuentan con un *servidor* que lleva a cabo la tarea de enviar cada trabajo a la impresora de turno. La función del servidor de impresión puede llevarse a cabo de diferentes maneras:

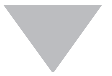
- Mediante un servidor de archivos con una impresora conectada directamente a él. (En general, esta opción no se recomienda ya que puede afectar adversamente el desempeño del servidor de archivos).
- Mediante una computadora conectada a la red, con una impresora conectada a ella. La computadora trabaja con un software especial para servidores de impresora para llevar a cabo esta tarea.

- Mediante el uso de un servidor de impresora incluido en la tarjeta de interfase de red (NIC) de la impresora. Por ejemplo, casi todas las LaserJet de Hewlett-Packard ofrecen una opción que permite instalar una tarjeta de red en la impresora, la cual contiene el hardware necesario para trabajar como un servidor de impresión. Dicha tarjeta es mucho menos costosa que dedicar una computadora independiente para llevar a cabo este trabajo.
- ▲ Por medio del uso de un servidor de impresión de red dedicado, que es una caja de aproximadamente el tamaño de un mazo de cartas que se conecta al puerto paralelo USB de la impresora (o también una conexión inalámbrica 802.11a u 802.11b) en un extremo y la red en el otro. Los servidores de impresión dedicados también contienen el hardware necesario para trabajar como éstos.

Servicios de aplicación

De la misma forma en que usted puede compartir archivos en una red, con frecuencia también puede compartir aplicaciones. Por ejemplo, si posee el tipo de licencia de software, puede tener una copia compartida de Microsoft Office, o alguna otra aplicación, y conservarla en el servidor de la red, desde donde también puede trabajar con dicha copia. Cuando una estación de trabajo desea correr el programa, carga los archivos desde la red en su propia memoria, de la misma manera que lo haría desde un disco local y corre el programa como de costumbre. Mantener las aplicaciones en un punto central reduce la cantidad de espacio en disco necesario en cada estación de trabajo y facilita la administración de la aplicación. (Por ejemplo, en algunas aplicaciones solo tiene que actualizar la copia de la red; en otras, también debe hacer una pequeña instalación en cada cliente).

Otro servicio de aplicación que puede tener en la red es un punto de instalación compartido para aplicaciones. En lugar de tener que cargar un CD-ROM en cada estación de trabajo, usted puede copiar el contenido del CD-ROM en una carpeta de un servidor y después correr el programa de instalación desde esa carpeta en cada estación de trabajo, lo cual permite que la instalación de las aplicaciones sea mucho más rápida y conveniente.



PRECAUCIÓN Asegúrese de que cualquier aplicación que instale en un servidor de red tenga la licencia adecuada. La mayoría de las licencias de software NO le permiten correr una aplicación en múltiples computadoras. Aun si usted necesita sólo una copia de la aplicación para configurar los archivos en el servidor, necesitará una licencia por cada usuario. Las diferentes aplicaciones sancionan con diferentes multas este tipo de maniobras. (Algunas requieren de una licencia por usuario, otras una licencia por computadora, otras permiten que sus usuarios de red utilicen libremente una copia en casa, etc.). Asegúrese de leer cuidadosamente los acuerdos de la licencia de su software de negocios y adhiérase a sus términos y condiciones.

Correo electrónico

Un recurso de red extremadamente valioso e importante en estos días es el correo electrónico. No solo puede ser muy útil para las comunicaciones dentro de su compañía, sino que también es el vehículo predilecto para comunicarse hacia el exterior de ella.

A grosso modo, los sistemas de correo electrónico se dividen en dos tipos: basados en archivos y cliente/servidor. El primero consiste en un conjunto de archivos que residen en una ubicación compartida en un servidor tipo el cual, en realidad, no hace nada más que proporcionar acceso a los archivos. Las conexiones que se requieren desde un sistema de correo electrónico de este tipo y el mundo exterior (digamos a Internet) son generalmente llevadas a cabo por una computadora independiente —llamada *servidor de compuerta*— que maneja la interfase de correo electrónico entre los dos sistemas mediante el software de compuerta que forma parte del sistema de correo electrónico basada en archivos.

Un sistema de correo cliente/servidor consta de un servidor de correo electrónico que contiene el mensaje y maneja todas las interconexiones de correo electrónico, tanto dentro de la compañía como fuera de ella. Estos sistemas, como Microsoft Exchange o Lotus Notes, son más seguros y mucho más poderosos que los basados en archivos. A menudo ofrecen características adicionales que le permiten utilizar el sistema de correo electrónico para automatizar diferentes procesos internos del negocio, como la facturación y las compras.

Salvo que la compañía cuente con 25 empleados, los servidores o los sistemas de correo electrónico están usualmente saturados y son costosos en precio y mantenimiento. Para estas pequeñas compañías, el correo electrónico también es importante, pero existen actualmente otras estrategias para ofrecer este servicio que no requieren que instale su propio sistema de correo electrónico interno (ya sea basado en archivos o cliente/servidor). Por ejemplo, muchas compañías pequeñas configuran simplemente cuentas de correo electrónico ya sea mediante su proveedor de servicios de Internet (ISP) o por medio de un servicio de correo electrónico sin costo como Yahoo! Mail o Hotmail. Alternativamente, usted puede correr Microsoft Windows Small Business Server 2003, el cual incluye una versión limitada de Exchange Server junto con otros paquetes de software que están diseñados para compañías pequeñas.

Acceso remoto

Otro servicio importante para la mayoría de las redes es el acceso remoto a los recursos de éstas. Los usuarios utilizan esta característica para acceder a sus archivos y a su correo electrónico cuando se encuentran de viaje o trabajan desde una ubicación remota, como un hotel o sus casas. Existen muchos tipos de sistemas de acceso remoto. Algunos de los métodos que se utilizan para proporcionar acceso remoto se basan en:

- Establecer una conexión simple de servicio de acceso remoto (RAS) en un Windows Server, que puede variar desde utilizar un solo módem hasta un banco de módems.
- Utilizar un sistema de acceso remoto dedicado, que maneje muchos módems y que generalmente incluya muchas computadoras, cada una en su propia tarjeta independiente.
- Emplear una estación de trabajo en la red y hacer que los usuarios marquen a ella mediante un programa de control remoto como PC Anywhere.
- Establecer una conexión de red privada virtual (VPN) a Internet, mediante la cual los usuarios pueden acceder a los recursos de la red de la compañía de manera confiable mediante Internet.
- Instalar Windows Terminal Services (sobre Windows Servers) o Citrix MetaFrame, los cuales permiten que un solo Windows Server administre múltiples sesiones de cliente, cada uno de los cuales aparenta ser una computadora independiente para el usuario final.

Como puede ver, existen muchas formas de proporcionar servicios de acceso remoto a los usuarios de la red. La solución correcta depende de qué necesiten los usuarios hacer remotamente, cuántos usuarios tienen (en total y en cualquier momento dado) y cuánto dinero quiere gastar. Consulte el capítulo 10 para obtener más información acerca del acceso remoto.

Redes de área amplia

Usted debe pensar en una red de área amplia (WAN) como un tipo de “metarred”. Una WAN es simplemente la conexión de varias redes de área local (LAN) entre sí. Este megasistema puede construirse de muchas formas en función de la frecuencia con que sea necesario conectar las LAN entre sí, cuánta capacidad de datos (ancho de banda) se requiere y cuál es la distancia entre las LAN. Las soluciones pueden variar desde utilizar líneas telefónicas privadas que puedan transportar datos a 56 Kbps, hasta líneas dedicadas DS1 (T-1) que transporten 1.544 Mbps o líneas DS3 que transporten 44.736 Mbps u otras soluciones (como satélites privados) que transporten anchos de banda aún mayores. Usted también puede instalar una WAN utilizando VPN mediante Internet, que aunque generalmente ofrece un ancho de banda inconsistente, a menudo es el menos costoso.

Las WAN se instalan cuando los usuarios de una LAN necesitan acceder con mucha frecuencia a los recursos de otra LAN. Por ejemplo, un sistema para la planeación de recursos de una compañía (ERP) puede operar en las oficinas centrales de ella, pero la ubicación de la bodega necesita acceder a él a fin de poder utilizar sus funciones de inventario y embarque.



CONSEJO Como regla general, si usted puede diseñar y construir una sistema que no requiera una WAN, será lo mejor ya que estos enlaces son a menudo costosos desde el punto de vista de su mantenimiento. Sin embargo, la estructura geográfica y de administración de una compañía en particular pueden dictar el uso de una WAN.

Internet e intranet

En estos días no cabe ni la menor duda: Internet se ha convertido en una herramienta vital para incrementar la productividad de la mayoría de los negocios. Por ello, manejar la conectividad en Internet en una red es, con frecuencia, un servicio muy importante. Existe un gran número de tipos de servicios que se ofrecen mediante Internet, entre ellos el correo electrónico, la web y los grupos de noticias de Usenet.

¡DEFÍNALO! xAN

Existe un gran número de términos que se refieren a las redes de área amplia (WAN), todos con variaciones en el esquema de siglas xAN. Algunos ejemplos de estas variaciones son red de área metropolitana (MAN), red de área a distancia (DAN), red de área de campus (CAN) y aun —no exagero— redes de área personalizada (PAN), la cual fue una demostración tecnológica de IBM donde dos personas que se dan la mano pudieron intercambiar datos a través de señales eléctricas transportadas sobre la superficie de su piel. Todos estos diferentes nombres y otros que no he mencionado aquí, son un poco ridículos. Sugiero que piense sólo en dos términos clave: LAN y WAN.

Una conexión a Internet de una red consiste en una conexión de una red de telecomunicaciones a un ISP mediante una conexión como una línea privada DSL, una línea ISDN o una conexión DS1 (T-1) fraccional o total. Esta línea entra al edificio y se conecta a una caja llamada CSU/DSU (unidad de servicio de canal/unidad de servicio de datos), la cual convierte los datos de la forma en que se transportan por medio de la compañía telefónica local a una forma que pueda utilizar la LAN. La CSU/DSU, a su vez, se conecta a un ruteador que direcciona los paquetes de datos entre la red local e Internet. La seguridad en Internet se ofrece ya sea mediante el filtrado de los paquetes que pasan a través del ruteador o, más comúnmente, por medio de la adición de un sistema de firewall. Un sistema de firewall opera en una computadora (o tiene una computadora incluida si es un dispositivo) y proporciona el nivel más alto de las funciones de seguridad y administración.

Una *intranet*, como su nombre lo sugiere, es una red con enfoque interno que imita a una red Internet. Por ejemplo, una compañía puede utilizar una intranet que tenga un servidor de web, en el cual la compañía puede colocar documentos como los manuales de los empleados, formatos de compra y cualquier otra información que publique para uso interno. Las intranets pueden también ofrecer otros servicios como los FTP o los Usenet, u ofrecerlos a través de otras herramientas que proporcionen la misma funcionalidad. En general, las intranets no se pueden acceder desde un punto fuera de la LAN (aunque sí es posible) y sólo son una versión mucho más pequeña de la Internet que una compañía instala para su propio uso.

El conocimiento de estas tecnologías, servicios y características de la red Internet es algo complejo. En el capítulo 6 usted podrá aprender más acerca del hardware que hace que Internet funcione.

Seguridad de la red

Siempre que comparta información confidencial o importante a través de una red, tiene que considerar muy cuidadosamente la seguridad de esos recursos. Tanto los usuarios como la alta dirección deben proporcionar ayuda a fin de configurar el nivel de seguridad necesario de la red y de la información almacenada en ésta, así como participar en la decisión respecto de quiénes tendrán acceso a qué recursos.

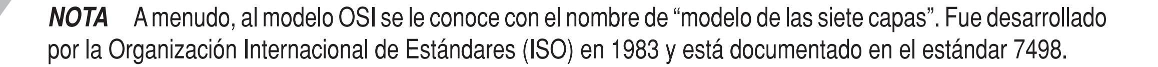
La seguridad de la red se brinda por medio de una combinación de factores, dentro de los que se incluyen las características del NOS, la planta física del cableado, cómo se conecta la red a otras redes, las características de las estaciones de trabajo cliente, las acciones de los usuarios, las políticas de seguridad de la dirección y con qué eficiencia se deben implantar y administrar las características de seguridad. Todos estos aspectos forman una cadena, por lo cual una falla en cualquier enlace de la misma puede provocar que falle la red en su totalidad. Dependiendo de la compañía, cualquier falla en la seguridad de la red puede tener consecuencias severas, por lo que la seguridad es, en general, una parte extremadamente importante de cualquier red. Consulte el capítulo 11 para conocer un análisis más detallado acerca de la seguridad en las redes.

EL MODELO DE INTERCONEXIÓN OSI

El modelo de interconexión para sistemas abiertos (OSI) define todos los métodos y protocolos necesarios para conectar una computadora a cualquier otra para formar una red. El modelo OSI es un modelo conceptual que se utiliza con mucha frecuencia para diseñar redes y elaborar la in-

geniería de las soluciones de red. En general, el modelo OSI conforma las redes en el mundo real, aunque existen diferencias entre la teoría que los sustenta y la práctica real en la mayoría de las redes. Aun así, este modelo proporciona una forma excelente para comprender y visualizar cómo se comunican las computadoras entre sí, y es un conocimiento indispensable para cualquier persona que trabaje en el campo de la conectividad de redes. Casi todas las compañías esperan que los profesionales en este campo tengan conocimientos acerca del modelo OSI, pues éste define una estructura básica de cómo funcionan las redes modernas. Dicho modelo también forma una parte clave de la mayoría de los exámenes para obtener la certificación en conectividad de redes. ¡Puede ser un poco árido, pero es importante aprenderlo!

El modelo OSI divide los métodos y protocolos necesarios en una conexión de red en siete diferentes capas. Cada capa superior depende de los servicios que ofrece la capa del nivel inferior. Para ilustrar este punto, si fuéramos a pensar en una computadora de escritorio, su hardware conformaría la capa más baja y los controladores del sistema operativo —la capa siguiente— dependerían de la capa inmediatamente inferior para hacer su trabajo. El sistema operativo por sí mismo, la capa superior siguiente, dependería de que las dos capas inferiores realizaran su función adecuadamente. Este esquema continúa de la misma forma hasta el punto en el que una aplicación le presenta datos al usuario desplegados en la pantalla. La figura 3-3 muestra las siete capas del modelo OSI.



NOTA A menudo, al modelo OSI se le conoce con el nombre de "modelo de las siete capas". Fue desarrollado por la Organización Internacional de Estándares (ISO) en 1983 y está documentado en el estándar 7498.

Figura 3-3. Las siete capas del modelo OSI.

Para una conexión de red completa, los datos fluyen de la capa superior hasta la inferior de una de las computadoras y luego, a través del cable que las conecta y después a través de las siete capas de la otra computadora. Las secciones siguientes analizan cada capa, comparándolas con sistemas reales de conectividad de redes cuando es apropiado.

Capa física

La primera capa, la *capa física*, define las propiedades del medio físico de transmisión que se utiliza para llevar a cabo la conexión de la red. Las especificaciones de la capa física se resumen en un medio físico de transmisión —un cable de red— que transmite un flujo de bits entre los nodos a través de la red física. La conexión física puede ser punto a punto (entre dos puntos) o multipunto (entre muchos puntos, de un punto a muchos otros), y puede consistir en transmisiones *half-duplex* (en una dirección a la vez) o *full-duplex* (en ambas direcciones simultáneamente). Además, los bits pueden transmitirse ya sea en serie o en paralelo. (La mayoría de las redes utilizan una ráfaga serial de bits, pero el modelo OSI permite ambos tipos). La especificación de la capa física también define el cable que debe utilizarse, los voltajes en el cable, la temporización de las señales eléctricas, la distancia que puede soportar, etc. Por ejemplo, una NIC es parte de la capa física.

Capa de enlace de datos

La *capa de enlace de datos*, o capa dos, define los estándares que asignan un significado a los bits que transporta la capa física. Establece un protocolo confiable a través de la capa física a fin de que la capa de red (capa tres) pueda transmitir sus datos. La capa de enlace de datos típicamente detecta y corrige los errores para asegurar una flujo de datos confiable. A los elementos de datos que transporta la capa de enlace de datos se les llama *tramas*. Algunos ejemplos de tramas típicas son la X.25 y 802.x (802.x incluye tanto a las redes Ethernet como Token Ring).

La capa de enlace de datos se divide generalmente en dos subcapas, llamadas control de enlace lógico (LLC) y control de acceso al medio (MAC). Si se utilizan, la subcapa LLC lleva a cabo tareas como establecer y terminar una llamada (el modelo OSI puede aplicarse tanto en redes de telecomunicaciones como en las LAN) y transferir datos. La subcapa MAC es responsable del ensamblado y desensamblado de las tramas, la detección y corrección de errores y el direccionamiento. Los dos protocolos MAC más comunes son el 802.3 Ethernet y el 802.5 Token Ring. Otros protocolos MAC son el 802.12 100Base-VBG, el 802.11 Wireless y el 802.7 Broadband.

En la mayoría de los sistemas, los controladores de las NIC llevan a cabo el trabajo que la capa de enlace de datos realiza.

Capa de red

La *capa de red*, o capa tres, es donde se produce mucha acción en la mayoría de las redes. Esta capa define la forma en que los paquetes de datos llegan de un punto a otro en la red y lo que va dentro de cada paquete. Además, define los diferentes protocolos de paquete, como el Protocolo Internet (IP) y el Protocolo de intercambio de Internet (IPX). Estos protocolos de paquetes incluyen información sobre enrutamiento fuente y destino. La información de enrutamiento que contiene cada paquete le dice a la red dónde enviarlo para que llegue a su destino, a la vez que le comunica a la computadora receptora dónde se originó dicho paquete.

Esta capa es particularmente importante cuando la conexión de red pasa a través de uno o más *ruteadores*, los cuales son dispositivos de hardware que examinan cada paquete y, a partir de

sus direcciones de origen y destino, envía los paquetes a su destino correspondiente. En una red compleja, como la Internet, un paquete puede pasar a través de diez o más ruteadores antes de llegar a su destino. En una LAN, es posible que un paquete no viaje a través de ningún ruteador a su destino o puede pasar a través de uno o más.

Observe que la descomposición de la capa de red (también conocida como *capa de paquete*) en una capa diferente a partir de las capas física y de enlace de datos, significa que los protocolos definidos en esta capa pueden viajar sobre cualquier variación de las capas inferiores. Por tanto, para poner lo que decimos en términos reales, un paquete IP puede enviarse mediante una red Ethernet, una Token Ring o de un cable serial que conecte dos computadoras entre sí. Lo mismo es válido para un paquete IPX: si ambas computadoras pueden manejar IPX, y comparten las capas del nivel más inferior (cualquiera que éstas sean), entonces puede establecerse una conexión de red entre ellas.

Capa de transporte

La *capa de transporte*, o capa cuatro, administra el flujo de información desde un nodo de red hasta otro. Se asegura de que los paquetes sean decodificados en la secuencia correcta y que se reciban todos. Asimismo, identifica de manera única a cada computadora o nodo en la red. Los diferentes sistemas de conectividad de redes (como el de Microsoft o Novell) tienen implantada la capa de transporte de una manera distinta y, en realidad, la capa de transporte es la primera capa donde se presentan entre los diferentes sistemas operativos de red. Sólo en esta capa se encuentran las redes Windows, Novell NetWare o cualquier otro sistema de conectividad de redes. Dentro de los ejemplos de protocolos de la capa de transporte se encuentran el Protocolo de control de transmisión (TCP) y el Intercambio Secuencial de Paquetes (SPX). Cada uno de ellos se utiliza en conjunto con IP e IPX, respectivamente.

Capa de sesión

La *capa de sesión*, o capa cinco, define la conexión de una computadora de usuario a un servidor de red y de una computadora a otra en una red con configuración de igual a igual. Estas conexiones virtuales se conocen como *sesiones*. Incluyen la negociación entre el cliente y el anfitrión, o de igual a igual, en aspectos como el control de flujo, el procesamiento de transacciones, la transferencia de información de usuario y la autentificación de la red.

Capa de presentación

La *capa de presentación*, o capa seis, toma los datos que le proporcionan las capas inferiores y los procesa a fin de que puedan presentarse al sistema (que es lo contrario a presentar los datos al usuario, lo cual se maneja fuera del modelo OSI). Dentro de las funciones que se llevan a cabo en la capa de presentación se encuentran la compresión y descompresión de datos, así como el cifrado y descifrado de los mismos.

Capa de aplicación

La *capa de aplicación*, o capa siete, controla la forma en que el sistema operativo y sus aplicaciones interactúan con la red. Las aplicaciones que se utilicen, como Microsoft Word o Lotus 1-2-3, no son parte de la capa de aplicación, pero proporcionan beneficios para el trabajo que se realiza ahí. Un ejemplo de software de la capa de aplicación es el software cliente que usted utilice, como el

Windows Client for Microsoft Networks, el Windows Client for Novell Networks o el software Client32 de Novell. Además, controla la forma en que el sistema operativo y las aplicaciones interactúan con dichos clientes.

Cómo viajan los datos a través de las capas del modelo OSI

Como se mencionó en esta sección, los datos fluyen desde un programa de aplicación o desde el sistema operativo y después se transfieren a través de los protocolos y dispositivos que conforman las diferentes capas del modelo OSI, uno por uno, hasta que llegan a la capa física y se transmiten a través de la conexión física de la red. La computadora en el extremo receptor invierte este proceso con los datos que llegan de la capa física, después los transfiere a través de todas las capas hasta que llega a la capa de aplicación donde son utilizados por el sistema operativo o por cualquiera de los programas de aplicación.

En cada etapa del modelo OSI, los datos son "encapsulados" con información de control relacionada con las funciones realizadas en esa capa en particular, pero deja intacta la información de las capas anteriores encapsuladas dentro de la nueva información de control. Esta información de control varía en cada capa, pero incluye *encabezados*, *información al final de la trama (trailers)*, *preámbulos* o *postámbulos*.

Así que, por ejemplo, cuando los datos viajan a través del software de conectividad y de los componentes que conforman el modelo OSI, comienza en la capa de aplicación e incluye un encabezado de la aplicación y datos de la aplicación (los datos que en realidad se envían). Después, en la capa de presentación, los datos encapsulan un encabezado de presentación que es transferido al componente en la capa de sesión, donde los datos encapsulan un encabezado de sesión, y así sucesivamente, hasta que llega a la capa física. Este proceso se invierte en la computadora en el extremo receptor, pues se desencapsula la información de control de cada capa, se realiza cualquier trabajo que indique esa información de control y se transfieren los datos a la capa superior inmediata. Todo esto suena como algo muy complejo; sin embargo, en la práctica no lo es.

COMPONENTES DE HARDWARE DE LA RED

En realidad, este capítulo trata acerca de la forma en que trabajan las redes, vista desde las alturas. En capítulos subsecuentes se analizará con más detalle la mayoría de los conceptos que se estudian en éste. Sin embargo, antes de pasar a los capítulos más detallados, es importante terminar este estudio mediante la presentación de un panorama del hardware específico que permite que las redes funcionen adecuadamente. La comprensión de los tipos de dispositivos en general que encuentra en una red es muy importante, no sólo para planear una red, sino también para repararla y proporcionarle mantenimiento.

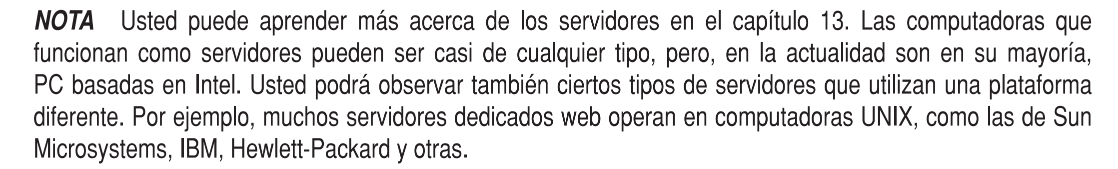
Servidores

Un *servidor* es cualquier computadora que lleva a cabo funciones de red para otras computadoras. Estas funciones se clasifican en varias categorías, dentro de las cuales están:

- Los servidores de archivo e impresión, que proporcionan la compartición de archivos y los servicios para compartir las impresoras basadas en la red.

- Los servidores de aplicación, que ofrecen servicios de aplicación específica a una aplicación. Un ejemplo es un servidor que maneje una base de datos que utilice una aplicación distribuida.
- Los servidores de correo electrónico, que ofrecen el almacenamiento del correo electrónico y los servicios de interconexión para las computadoras cliente.
- Los servidores de conectividad de redes, que proporcionan una gran variedad de diferentes servicios de red. Dentro de dichos servicios se encuentran la asignación automática de direcciones TCP/IP (servidores DHCP), enrutamiento de paquetes de una red a otra (servidores de enrutamiento), cifrado/descifrado y otros servicios de seguridad, servidores VPN y otros por el estilo.
- Los servidores de Internet, los cuales proporcionan servicios de la Web, de Usenet News (NNTP) y de correo electrónico a través de Internet.
- Los servidores de acceso remoto, que proporcionan acceso a una red local para los usuarios remotos.

Por lo general, los servidores corren algún tipo de NOS, como el Windows Server 2003, el Novell NetWare o UNIX. Dependiendo del NOS que se seleccione, la totalidad de las funciones que se mencionaron anteriormente podrían correrse en un servidor o estar distribuidas en muchos servidores. De la misma forma, no todas las redes necesitan todos los servicios que se mencionaron previamente.



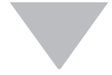
NOTA Usted puede aprender más acerca de los servidores en el capítulo 13. Las computadoras que funcionan como servidores pueden ser casi de cualquier tipo, pero, en la actualidad son en su mayoría, PC basadas en Intel. Usted podrá observar también ciertos tipos de servidores que utilizan una plataforma diferente. Por ejemplo, muchos servidores dedicados web operan en computadoras UNIX, como las de Sun Microsystems, IBM, Hewlett-Packard y otras.

Varias características distinguen una verdadera computadora tipo servidor de una computadora cliente común y corriente. Dentro de ellas se encuentran la redundancia integrada con fuentes de poder y ventiladores múltiples (por ejemplo), para mantener el servidor en funcionamiento en caso de una falla. También se incluyen diseños especiales de gran desempeño de los subsistemas de disco, memoria y red a fin de optimizar la transferencia de los datos desde y hacia el servidor, la red y las computadoras cliente. Por último, a menudo se incluye software y hardware especial de supervisión que se encarga de mantener al servidor en estado óptimo de operación, es decir, previene las fallas antes de que se presenten. Por ejemplo, la mayoría de los servidores tienen monitores de temperatura integrados; si la temperatura comienza a elevarse, se genera una alarma a fin de que el problema pueda ser resuelto antes de que provoque una falla en cualquiera de los componentes de hardware del servidor.

Concentradores, ruteadores y switches

Los concentradores, los ruteadores y los switches son el hardware de conectividad "puro" que se ve con más frecuencia. (Son "puros" en el sentido de que sólo se utilizan en la conectividad de redes sin algún otro propósito). La mayoría de las personas se refieren a este tipo de equipo como "dispositivos de conectividad de redes", ya que para ello sirven. Éstos son los dispositivos a los

que se conectan todos los cables de la red y que transportan los datos a través de las capas física, de enlace de datos y de red del modelo OSI.



NOTA En el capítulo 6 se estudian los concentradores, ruteadores y switches con más detalle, junto con otro hardware de conectividad de redes.

Un *hub*, a menudo llamado *concentrador*, es un dispositivo que conecta un gran número de cables de red provenientes de las computadoras cliente a una red. Los concentradores pueden ser de tamaños muy variados y pueden soportar desde dos computadoras hasta grandes concentradores a los que pueden conectarse 60 computadoras o más. (El tamaño del concentrador más común soporta 24 conexiones de red). Todas las conexiones de red de un concentrador comparten un *dominio de colisiones* único, lo cual es una forma graciosa de decir que todas las conexiones de un concentrador "hablan" a través de un único alambre lógico y están sujetas a interferencia por parte de otras computadoras conectadas al mismo concentrador. La figura 3-4 muestra el ejemplo de un concentrador y la forma en el que está alambrado lógicamente.

Un *switch* se cablea de forma muy similar a un concentrador y en realidad su apariencia es la de un concentrador. Sin embargo, en un switch, todas las conexiones de red se encuentran en su propio dominio de colisión. El switch hace que cada conexión de red sea privada y después reúne los datos de cada una de ellas y los transfiere a la espina dorsal de una red, que opera usualmente a una velocidad mucho más elevada que las conexiones individuales del switch. Con mucha frecuencia los switches se utilizan para conectar una gran cantidad de concentradores a una sola espina dorsal de red. La figura 3-5 muestra una configuración de cableado típica de un concentrador y un switch.

Un *ruteador* direcciona los paquetes de datos de una red a otras. Las dos redes se conectan al ruteador mediante su propio tipo de conexión y cableado. Por ejemplo, un ruteador que conecta a una red 10Base-T con una línea telefónica ISDN tendría dos conexiones: una que va a la red 10Base-T y otra que va a la línea ISDN proporcionada por la compañía telefónica. A menudo, los ruteadores también tienen una conexión adicional a la que puede conectarse una terminal; esta conexión sólo se utiliza para programar y proporcionar mantenimiento al ruteador.

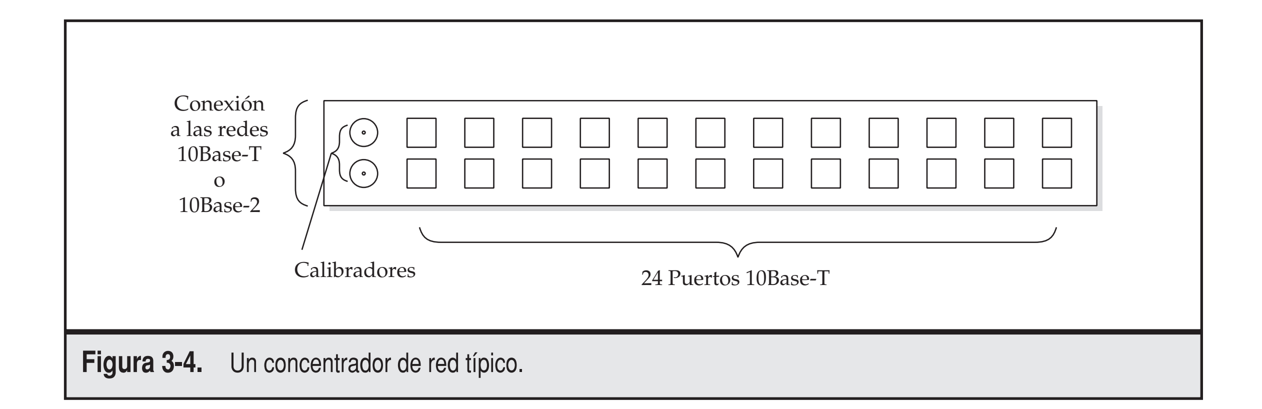


Figura 3-4. Un concentrador de red típico.

Figura 3-5. Utilización de switches y concentradores en una sola red.

Plantas de cable y de cableado

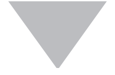
Existen muchos tipos de cables de red, pero sólo algunos de los más comunes son de interés. El cable de red más común para las LAN es el cable de par trenzado categoría 5 (Cat-5). Este cable transporta la señal de la red a cada punto a través de cuatros alambres (dos pares trenzados). El cable Cat-5 se utiliza en las redes Ethernet 100Base-T.



NOTA El trenzado de cada uno de los pares dentro del forro del cable reduce la probabilidad de que el cable sea afectado por la interferencia eléctrica.

En ocasiones podrá observar que se utiliza un cable de menor grado llamado cable categoría 3 (Cat-3). Éste es similar al cable Cat-5, pero tiene la mitad de alambres y utiliza conectores más

pequeños (aunque son los conectores modulares tipo teléfono). El cable Cat-3 se utiliza en redes 10Base-T. Mientras que el Cat-3 existente todavía proporciona un buen servicio, es muy raro verlo instalado, ya que muchas compañías han optado por actualizar el cableado de sus redes con Cat-5 o lo instalaron desde el principio, aun cuando sus redes utilizaban 10Base-T. (Es posible instalar una conexión de red con Cat-3 sobre una con Cat-5 y, debido a eso, muchas compañías instalaron un cable de grado mayor a pesar de que no lo necesitaban es ese momento, ya que el costo de volver a cablear todo el edificio es muy elevado).



NOTA En años más recientes, el cable Cat-5 ha experimentado mejoras y se le conoce como Cat-5E. También ha sido aprobado un estándar aún más novedoso llamado Cat-6. Tanto el Cat-5E como el Cat-6 son, en esencia, los mismos que el Cat-5, pero éstos cumplen con especificaciones de mayor calidad para manejar velocidades de red más elevadas.

El cable coaxial (llamado *coax*) no se utiliza en la actualidad en instalaciones nuevas de cableado, pero usted lo puede encontrar en edificios más antiguos. El cable coaxial tiene un núcleo central de cobre (llamado *conductor*) rodeado de una cubierta de plástico, que a su vez está envuelto con una protección metálica, llamada *revestimiento* y, por último, con una cubierta de plástico. Por ejemplo, el cable que utiliza para conectar una televisión a una red de TV por cable es un tipo de cable coaxial (por cierto, el mismo cable coaxial se utiliza en los módems por cable). La mayoría del cable coaxial que se emplea en las redes es del tipo RG-58, el cual se utiliza en redes 10Base-2 (Thin Ethernet). Otro es el RG-56, que se usa en redes ARCnet. Los diferentes tipos de cable coaxial se refieren a las especificaciones del cable, las cuales determinan si un tipo de red en particular puede utilizar el cable. Usted no puede mezclar diferentes tipos de cable coaxial en una sola red, y debe utilizar el tipo de cable correcto en la red que esté instalando.



NOTA Para obtener más información acerca del cableado de las redes consulte el capítulo 4.

El término *planta de cableado* se refiere a la instalación de todo el cable de red. Esto no sólo incluye el cable instalado en todo el edificio, sino también los conectores, placas instaladas sobre la pared, paneles de conexión y otros por el estilo. Es de primordial importancia que la instalación de la planta de cableado en un edificio sea realizada por un contratista calificado que esté entrenado para instalar ese tipo de cable. A pesar de la apariencia simple del cable, en realidad es muy complejo, así como también su instalación.

Hardware de las estaciones de trabajo

Cualquier computadora de una red que sea utilizada por los usuarios se conoce, en general, como una *estación de trabajo de la red*. A veces, dichas estaciones de trabajo también se conocen como *clientes de red*. En general, un cliente de red es una PC con tecnología Intel que trabaja con alguna versión de Windows, la cual tiene instalada una NIC junto con algún software cliente de red, que permite que la estación de trabajo pueda operar en la red. Las estaciones de trabajo de la red también pueden ser cualquier otro tipo de computadora que tenga el software y hardware de red necesarios, por ejemplo la Macintosh, de Apple, o algún tipo de computadora UNIX.



PISTA No confunda una estación de trabajo de red (un término genérico) con las computadoras tipo estación de trabajo. Estas últimas son computadoras que se utilizan en el diseño asistido por computadora, en ingeniería y en el trabajo con gráficas.

RESUMEN DEL CAPÍTULO

En este capítulo se presentó un gran número de conceptos importantes acerca de la conectividad de redes. Usted aprendió acerca de cómo se relacionan entre sí las computadoras conectadas a través de una red, cómo se dividen lógicamente las diferentes partes de una conexión de red en el modelo de red OSI, y de qué manera este modelo es de utilidad para comprender las redes. Asimismo, aprendió acerca de un gran número de características y recursos básicos de las redes.

Los capítulos siguientes abordan estos temas con más detalle, comenzando en el capítulo siguiente, en el cual se analiza el a menudo incomprendido mundo del cableado de las redes.



CAPÍTULO 4

Cableado de las redes

Si usted compara una red de computadoras con el cuerpo humano, el sistema de cableado de la red serían los nervios que conforman el sistema nervioso. El sistema de cableado es lo que en realidad transporta los datos de un punto a otro y determina cómo trabaja la red. La forma en que está cableada la red es de primordial importancia para determinar su funcionamiento, su rapidez y su confiabilidad, considerándola como un todo, así como la facilidad para expandirla o modificarla. Lo primero que se debe hacer después de evaluar las necesidades de la red es determinar cómo deberá cablearse; todos los demás componentes se construirán sobre esa base. Este enfoque se parece mucho al modelo OSI de siete capas que se estudió en el capítulo 3, en el sentido de que el cableado de la red conforma la capa uno, la capa física, y las capas superiores dependen de ella.

Muchas personas piensan que el cableado de la red es relativamente sencillo. Después de todo, ¿qué puede ser más simple que instalar un cable entre dos puntos? Sin embargo, como usted verá, el tema del cableado de las redes abarca más de lo que piensa y es un área muy importante que debe hacerse correctamente. Si comete errores en la selección o instalación del cable de la red, es muy probable que ésta no sea confiable y que tenga un desempeño muy bajo. Debido a los costos de mano de obra que implica el cableado, el mejor momento para reparar cualquier problema potencial en esta área es mucho antes de que se presente.

TOPOLOGÍAS DEL CABLEADO

La palabra *topología* significa, básicamente, *forma*; el término *topología de red* se refiere a la forma de una red, es decir, a cómo están cableados todos los nodos (puntos) de una red. Existen varias topologías con las que están cableadas las redes y la selección de una en particular es, a menudo, la decisión más importante cuando está planeando una red. Las diferentes topologías tienen costos (tanto la instalación como el mantenimiento), niveles de desempeño y niveles de confiabilidad muy variados. En las secciones siguientes aprenderá acerca de las principales topologías que se utilizan.

¡DEFÍNALO! Segmento de red

El significado de un segmento de red puede variar de acuerdo con la topología de la misma, pero el concepto es más sencillo en el caso de las redes tipo *bus* y es, en esencia, la misma para cualquier otra topología. Un segmento es un tramo de cable al que se conectan todos los nodos; en realidad, no es un tramo continuo de cable ya que se rompe en cada punto de conexión de las computadoras de la red a través de un conector que permite la conexión del nodo al cable de la misma, pero el cable es, eléctricamente, un tramo completo. Es necesario que tome esto en cuenta cuando planee cómo se conectarán muchos nodos a cualquier segmento. Si usted tiene 20 computadoras que utilizan ese segmento al mismo tiempo, cada computadora podrá utilizar aproximadamente 1/20avo. del ancho de banda máximo disponible. Esto es una simplificación; usted aprenderá más acerca de cómo funciona todo esto en este capítulo y en los siguientes.

Topología bus

Una *topología bus*, también conocida como *Topología bus común multipunto*, es una red donde se utiliza un solo cable que corre desde un extremo al otro de la red y que tiene diferentes dispositivos (llamados *nodos*) de red conectados al cable en puntos diferentes. La figura 4-1 muestra una red con topología bus.

Los diferentes tipos de red en bus tienen distintas especificaciones, las cuales incluyen los factores siguientes:

- Cuántos nodos puede tener un solo segmento.
- Cuántos segmentos se pueden tener si se utilizan repetidores.
- Cuán cercanos pueden estar los nodos entre sí.
- La longitud total de un segmento.
- Qué tipo de cable coaxial se requiere.
- Cómo deben terminarse los extremos del bus.

En estos días las instalaciones del cableado de las redes rara vez utilizan las topologías en bus, aunque algunas más antiguas lo hacían. Las redes con esta topología utilizan cable coaxial, el cual se describió en el capítulo anterior. Cada extremo de un segmento de la red tiene conectado un terminador especial, sin el cual la red no funcionaría. Las redes con topología bus utilizan conectores BNC para unir los diferentes pedazos de cable. Cada computadora se conecta a la red por medido de un conector BNC tipo T (así llamado por tener la forma de la letra T) que permite la continuidad del bus y que la computadora se conecte a él. La figura 4-2 muestra diferentes tipos de conectores BNC.

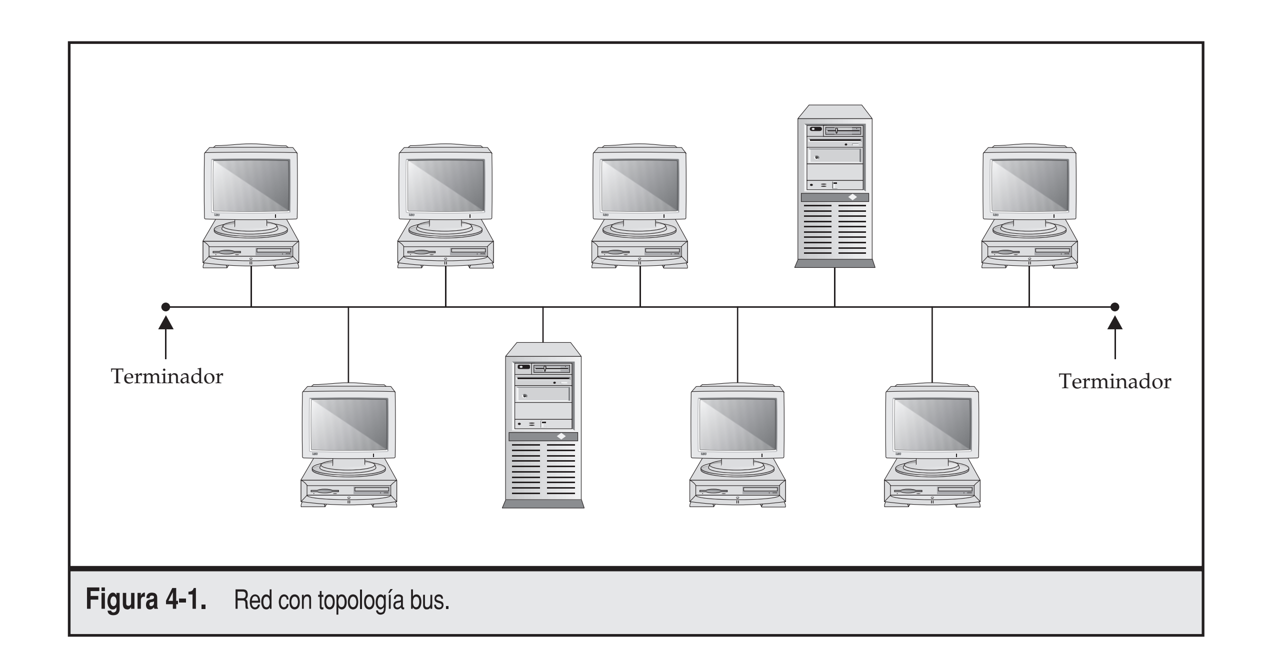


Figura 4-1. Red con topología bus.

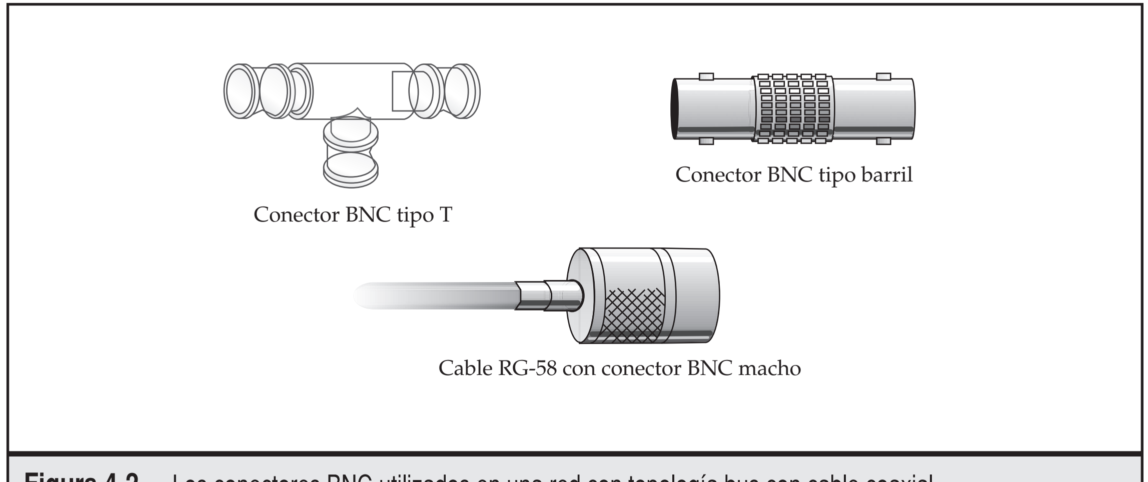


Figura 4-2. Los conectores BNC utilizados en una red con topología bus con cable coaxial.

Las topologías bus son las más económicas debido a que utilizan mucho menos cable que las otras dos topologías y, por tanto, emplean menos material y necesitan menos mano de obra para su instalación.

Sin embargo, las redes con topología bus tienen grandes desventajas. Debido a que todos los subcables que conforman el segmento y corren de un nodo a otro deben estar conectados en todo momento, una falla en cualquier parte del segmento provocará la falla de todo. Y aún más importante, toma mucho tiempo rastrear este problema ya que debe realizar pruebas en todas las conexiones del cable hasta que encuentre la que causa el problema. A menudo, la fuente del problema no se puede ver a simple vista, por lo que debe utilizar diferentes técnicas y equipo para rastrear el problema. Debido a la tendencia de las redes con topología bus a ser poco confiables, ya casi no se utilizan en las redes actuales.

¡DEFÍNALO! Conectores BNC

Según a quién le pregunte, las siglas BNC significan Bayounet Nut Connector, British Naval Connector o Bayonet Nelly-Concelman (donde las últimas dos palabras forman el nombre de su inventor, Mr. Nelly-Concelman). El BNC es un conector tipo bayoneta que se conecta y desconecta de manera muy rápida con un cuarto de vuelta. Una gran variedad de partes —conectores tipo T, conectores tipo barril, conectores tipo codo, extremos de cables que se empalman en el cable apropiado, etc.— utilizan conectores BNC, por lo que usted puede realizar cualquier tipo de conexión que necesite. El conector BNC es extremadamente fácil de hacer y se obtienen conexiones muy seguras con él.

En definitiva, la red tipo bus que prevaleció en el pasado se llama 10Base-2 Ethernet o, comúnmente, Thin Ethernet. Este tipo de red tiene las características siguientes:

- Opera a una velocidad máxima de 10 Mbps.
- Utiliza cable coaxial tipo RG-58/AU o RG-58/Cu y conectores BNC.
- Para funcionar, requiere un conector terminador de 50 ohms en cada uno de los extremos del segmento.
- Puede manejar un máximo de 30 nodos por segmento.
- La longitud de segmento máxima que puede instalarse es de 185 metros (607 pies).
- Puede utilizar segmentos extendidos mediante el uso de repetidores. Si éstos se van a utilizar, usted puede conectar un máximo de tres segmentos, y cada uno puede tener hasta 30 nodos (donde el repetidor cuenta como un nodo). Usted también puede tener dos segmentos adicionales (un total de cinco), si esos dos segmentos extra se utilizan sólo para incrementar la distancia, sin que se les puedan conectar nodos. Un segmento completo con repetidores nunca deberá exceder un total de 925 metros (3035 pies). Recuerde la regla 5-4-3: cinco segmentos, cuatro repetidores, tres segmentos con nodos.
- Requiere que cada nodo se encuentre a una distancia de, al menos, 1.5 pies (distancia del cable) de cualquier otro nodo.



NOTA Los repetidores son dispositivos de hardware que aumentan el nivel eléctrico de la señal que viaja a través del cable, por lo que puede extenderse aún más; no proporcionan enrutamiento de datos. En realidad, un repetidor "ignora" los datos que pasan por él y son baratos y confiables. Sin embargo, recuerde que un cable extendido por medio de un repetidor significa que todo el tráfico de la red en un lado del mismo es reflejado en el cable del otro lado, sin importar si ese tráfico necesita viajar a través de ese otro cable.

Topología estrella

La *topología estrella* es una en la que una unidad central, llamada *hub* o *concentrador*, trabaja como punto de conexión para enlazar cada nodo de la red. En términos técnicos, al concentrador se le conoce como unidad de acceso multiestación (MAU), pero esa terminología en particular tiende a utilizarse sólo en las redes Token Ring, las cuales usan una topología lógica en anillo (consulte la sección siguiente). Por lo general, cada concentrador puede conectar aproximadamente 24 nodos, aunque existen concentradores que varían en tamaño desde 2 hasta 96 nodos. Sin importar su tamaño, usted puede conectar múltiples concentradores entre sí para expandir una red de cualquier forma que tenga sentido. Consulte el capítulo 6 para obtener mayor información acerca de la conexión de concentradores con configuraciones diferentes. La figura 4-3 muestra una red sencilla con topología estrella.

Todo el tráfico que viaja de cualquier conexión de la red al concentrador se difunde a todos los demás nodos conectados a ese concentrador. Debido a esto, todo el ancho de banda de cualquier conexión a los nodos se comparte con todas las demás. Por ejemplo, si uno de los nodos conectados a la red utiliza la mitad del ancho de banda disponible, todos los demás nodos deberán disputarse el uso de ese ancho de banda. En otras palabras, si usted utiliza una red de este tipo a una capacidad de 10 Mbps, este valor representa el ancho de banda total disponible por todos los nodos conectados al concentrador.

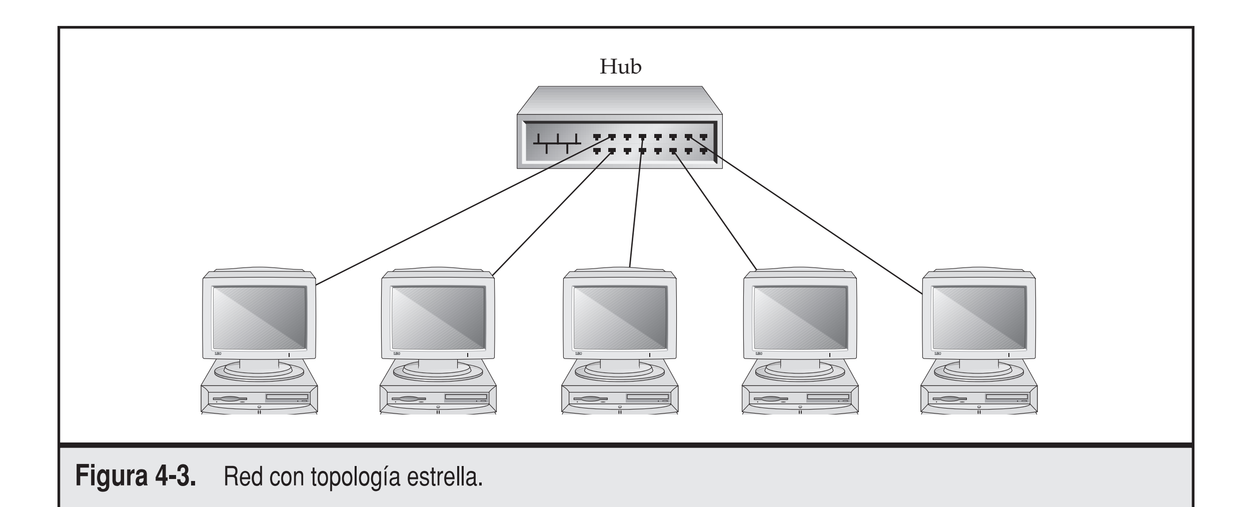


Figura 4-3. Red con topología estrella.

NOTA Las redes cableadas físicamente con una topología estrella pueden ser un bus o un anillo lógico. Ello significa que, independientemente de cómo se vea la red, aún se "comporta" como un bus o un anillo. Las redes Ethernet cableadas en forma de estrella representan un bus lógico, mientras que las redes Token Ring cableadas en forma de estrella son un anillo lógico.

Las redes con topología estrella puede utilizar una o varias formas de Ethernet. La más común es la 100Base-T Ethernet, la cual tiene 100 Mbps de ancho de banda. Asimismo, existen sólo algunas redes más antiguas que utilizan 10Base-T Ethernet, la cual ofrece 10 Mbps de ancho de banda. Un estándar más novedoso, llamado Gigabit Ethernet (1 000 Base-T), brinda 1 Gbps de ancho de banda. Un nuevo estándar ha sido aprobado recientemente, que se llama 10 Gigabit Ethernet (o, también llamado 10GBase-X), puede operar a 10 Gbps a través de fibra óptica.

¡DEFÍNALO! Físico contra lógico

A menudo escuchará hablar de los términos "físico" y "lógico" cuando estudie sobre redes. Estos términos se emplean para definir cosas diferentes. La palabra físico, que se utiliza en el contexto de la conectividad de las redes, se refiere al aspecto físico, real, esto es, lo que se puede ver y sentir. La palabra lógico se refiere a la forma en que algo trabaja, a pesar de su apariencia. Por ejemplo, una red Token Ring se cablea físicamente en estrella; cada cable se extiende del MAU a cada uno de los nodos. Sin embargo, lógicamente, es un anillo a través del cual las señales viajan de un nodo a otro de forma circular. El hecho de que las señales viajen físicamente de un nodo al MAU y de regreso al nodo siguiente, en general no es importante cuando se piensa en el arreglo lógico circular de la red Token Ring.

10Base–T requiere un tipo de cable de par trenzado llamado Categoría 3 (Cat-3), mientras que 100Base-T requiere del cable Categoría 5 (Cat-5). 10Base-T también puede usar Cat-5, pero 100base-T no puede usar Cat-3; en estos días uno siempre debe usar el novedoso cable Cat-5 —llamado Cat-5E— incluso si sólo se utilizara en una red 10Base-T. (Si el costo no representa ningún problema, considere utilizar el Cat-6.)

Las redes 10Base-T comparten las características de cableado siguientes:

▼ En realidad requiere cuatro alambres (dos pares trenzados en un solo forro); puede ser par trenzado sin protección (UTP) o con protección (STP).

■ Puede instalarse con cable Cat-3 o Cat-5 (el cable Cat-5 tiene ocho alambres —cuatro pares trenzados—por lo que, si se desea, puede transportar el tráfico de dos conexiones en cada cable).

■ Está limitada a una longitud de 100 metros (328 pies) por cada conexión.

■ No está limitada en cuanto al número de nodos en un solo segmento lógico.

▲ Utiliza conectores RJ-45 en todas las conexiones. (Este tipo de conector es similar al conector telefónico modular, pero el RJ-45 es más grande).

Las redes 100Base-T son parecidas a las 10Base-T, pero tienen estas características:

▼ En realidad requieren cuatro alambres (dos pares trenzados en un mismo forro).

■ Deben utilizar cable Cat-5 o mejor.

■ Están limitadas a una longitud de 100 metros (328 pies) en cada conexión de nodo.

■ No existe límite en cuanto al número de nodos en un solo segmento lógico.

▲ Utilizan conectores RJ-45 en todas las conexiones.

Las redes 1 000Base-T se distinguen porque se instalan sobre el cable Cat-5 existente pero a una velocidad diez veces mayor que la de las redes 100Base-T. El hecho de que puedan operar sobre Cat-5 es una ventaja muy importante para las redes 1 000Base-T, ya que alrededor de 75% del cableado instalado en las redes en la actualidad es Cat-5, y volver a cablear todo un edificio a fin de actualizarse a un nuevo estándar de conectividad es una propuesta extremadamente costosa. La red 1 000Base-T que utiliza Cat-5 tiene estas características:

▼ Requiere ocho alambres (cuatro pares trenzados en un mismo forro).

■ Debe utilizar cable Cat-5 o mejor.

■ Está limitada a una longitud de 100 metros (328 pies) en cada conexión de nodo.

■ No existe límite en cuanto al número de nodos en un solo segmento lógico.

▲ Utiliza conectores RJ-45 en todas las conexiones.

Las redes con topología estrella tienen dos desventajas implícitas en comparación con las redes en bus. Primero, son más costosas. Es necesaria una mayor cantidad de cable, la mano de obra para cablearlas es mucho mayor y es necesario un gasto adicional debido al costo de los concentradores. Sin embargo, para contrarrestar estos costos, la topología estrella es mucho más

confiable que la topología bus. En la topología estrella, si falla una sola conexión de la red (está cortada o dañada de alguna forma), solo esa conexión resulta afectada. Mientras que es verdad que los concentradores repiten todas las señales de la red de los nodos conectados a ellos hacia los demás nodos, también tienen la capacidad de *partir* o cortar, de manera automática, cualquier conexión de red que no funcione correctamente —una manzana podrida no va a echar a perder a todas—. Además, debido a que cada cable está instalado directamente del nodo al concentrador, es extremadamente sencillo reparar una falla en la red; no tiene que buscar por todo el edificio dónde se encuentra el problema.

Topología anillo

La *topología anillo*, como usted podría imaginarlo, no es un arreglo físico de un cable de red. En lugar de eso, los anillos son un arreglo lógico: los cables están instalados en forma de estrella, en la que cada nodo está conectado al MAU con su propio cable. Sin embargo, eléctricamente las redes se comportan como un anillo, pues las señales circulan alrededor del anillo de nodo en nodo. La figura 4-4 muestra un ejemplo de una red con topología en anillo.

Las LANs con topología anillo se basan en Token Ring en lugar de Ethernet. Algunas de ellas pueden operar como interfase de datos distribuidos por fibra (FDDI) —una red a 100 Mbps por fibra óptica— en lugar de cable de cobre. Las redes en anillo también se utilizan en grandes redes de telecomunicaciones como la red óptica síncrona (SONET), así como en las redes de área de almacenamiento y en algunas otras aplicaciones.

Comparación de la topología anillo con las topologías estrella y bus

Para comprender cómo se compara la topología anillo con las topologías estrella y bus, usted necesita primero comprender cómo trabaja la red Ethernet. Estas redes manejan todas las señales en la red mediante el empleo de una técnica llamada CSMA/CD, que quiere decir acceso múltiple por sensado de portadora con detección de colisiones. CSMA/CD permite que cada nodo de un segmento transmita datos en el momento que desee. Si, por coincidencia, dos nodos tratan de transmitir al mismo tiempo, cada uno lo detectaría con su mecanismo de detección de colisiones, después, ambos nodos esperarían una cantidad de tiempo aleatoria (en milisegundos) para volver a intentar la transmisión.

Si usted piensa en cómo fluyen los paquetes de datos en una red cuando utiliza CSMA/CD, es probable que piense que rápidamente podría convertirse en un total desorden, ya que las retransmisiones de los datos y las colisiones provocarían aún más colisiones. Y probablemente pensaría que podría existir el riesgo potencial de que la red alcanzara un punto de saturación en el que no se pudiera transmitir ningún dato debido al exceso de colisiones en ella. Usted estaría en lo correcto. En la redes 10Base-T, este punto se presenta en las inmediaciones de los 3.5 Mbps (aproximadamente a un tercio de la velocidad teórica máxima de 10 Mbps que un nodo puede alcanzar al enviar datos a otro nodo). Sin embargo, por dos razones, la realidad es que las excesivas colisiones no representan un gran problema en la mayoría de las redes. Primero, la mayor parte del tráfico en la red es en *ráfagas*, y los nodos de la red muy raramente utilizan todo el ancho de banda, en una red en particular, en un periodo significativo. Segundo, aun en una red donde las excesivas colisiones afectaran su desempeño, es relativamente sencillo fragmentar el segmento de red en segmentos más pequeños y reducir proporcionalmente la probabilidad de colisión. En la realidad, la técnica CSMA/CD trabaja bien y Ethernet es el estándar de red que más ha predominado en el mundo debido a su alto desempeño y a su flexibilidad.

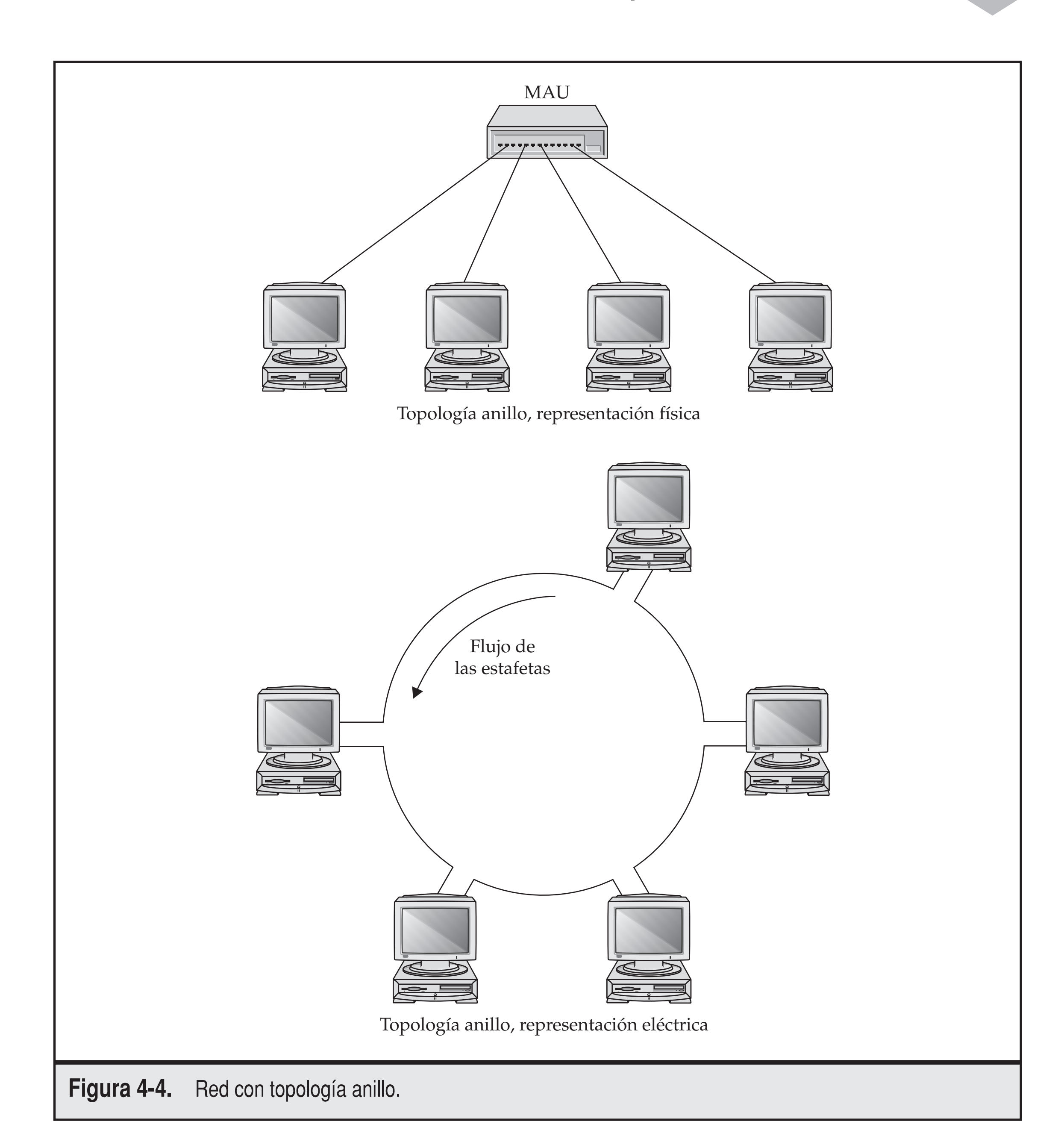


Figura 4-4. Red con topología anillo.

Las redes Token Ring trabajan bajo un principio diferente que las CSMA/CD, pues administran su ancho de banda con una técnica llamada *estafeta circulante*. Eléctricamente, una entidad de datos, llamada *estafeta*, circula alrededor del anillo lógico. La estafeta tiene dos estados: libre u ocupado. Cuando una estación desea transmitir datos, espera hasta que la estafeta que pase por su nodo se encuentre libre y, en ese momento, el nodo marca a la estafeta como ocupada. Después de colocar en la estafeta los datos que desea transmitir junto con la dirección de destino, el nodo envía el paquete al nodo siguiente. Este último, al ver que la estafeta se encuentra en estado ocupado, lee la dirección de destino y pasa la estafeta sin modificarla hacia éste. Una vez que el nodo de destino recibe la estafeta, obtiene sus datos, marca la estafeta como libre y la envía a la siguiente estación. Si en un momento dado la estafeta se "pierde", entonces una estación de trabajo genera, de manera automática, una nueva estafeta libre una vez que ha transcurrido un periodo determinado.

La belleza de las redes Token Ring reside en que su comportamiento es predecible a medida que aumentan las necesidades de los nodos. Asimismo, las redes Token Ring nunca se congestionan como resultado de colisiones, las cuales no se presentan en este tipo de redes. Sin embargo, los beneficios de las redes Token Ring se compensan con el ancho de banda que se desperdicia en el procesamiento necesario para administrar la estafeta. En resumen, las redes Token Ring tienen un desempeño tan rápido como las Ethernet con un ancho de banda similar.

IBM inventó la tecnología de las redes Token Ring a finales de los años sesenta y las primeras redes de este tipo comenzaron a aparecer en 1986. Mientras que muy pocas LAN Token Ring se encuentran instaladas (operando a 4 Mbps o 16 Mbps), se pueden encontrar predominantemente en compañías que tienen una relación muy estrecha con IBM y que, quizá, también utilicen una minicomputadora o una computadora grande marca IBM.

Si usted se encuentra diseñando una LAN, en general, su mejor opción es Ethernet con topología estrella. Encontrará que el equipo para esta red se encuentra disponible en el mercado, su precio es bajo y existe mucho personal calificado que puede instalar 100Base-T o 1 000Base-T. (No tiene mucho sentido instalar 10Base-T en estos días y, de hecho, el equipo no ya no se encuentra disponible en el mercado.) En redes nuevas, seleccione siempre cable Cat-5E, incluso cuando vaya a utilizar por el momento 100Base-T, de forma que tenga la posibilidad de actualizarla fácilmente a los estándares cambiantes.

Seleccione Token Ring si una necesidad externa lo obliga a hacerlo, como podría ser la necesidad de conectividad a una equipo grande IBM que no soporte Ethernet.

DESMITIFICACIÓN DEL CABLEADO DE LAS REDES

El cableado de las redes puede ser algo muy confuso. No sólo existe una gran diversidad de cables, todos con sus propios nombre y número, sino que, a menudo, puede seleccionar diferentes tipos de cable para instalarse en un solo tipo de red. Por ejemplo, las redes Ethernet pueden utilizar una cantidad sorprendente de tipos de cable que puede variar desde el coaxial hasta el cable de par trenzado con o sin protección, cable coaxial delgado o fibra óptica. Para diseñar y dar mantenimiento a cualquier tipo de red, necesita conocer cuáles son las opciones de cable y cómo proporcionarle mantenimiento.

El objetivo de esta sección es desmitificar los sistemas de cableado. Usted ha aprendido básicamente acerca de los tipos más comunes de cables para red, los tipos que encontrará en 99% de las redes instaladas y que se utilizarán en 99% de cualquier nueva red. Cuando convenga, en

esta sección se hará referencia a otros tipos de cable de manera que usted los conozca, pero es conveniente que enfoque su atención en sólo algunos tipos de cable que están instalados en la mayoría de las redes.

Tipos básicos de cable

Existen muchos tipos básicos de cable. Los más comunes son el par trenzado sin protección (UTP) y el coaxial, pero el UTP es el más común en la actualidad. Otros tipos de cableado de red son el par trenzado con protección (STP) y la fibra óptica.

El cable de par trenzado sin protección consiste en dos o más pares de conductores aislados con plástico dentro de un forro (hecho de vinyl o teflón). En cada par, los dos conductores se trenzan dentro del cable, lo cual ayuda a que soporte la interferencia eléctrica del exterior. Existen estándares acerca de cómo se fabrica este cable, los cuales especifican la distancia adecuada entre cada trenzado. La figura 4-5 muestra un ejemplo del cable UTP.

El cable STP es similar al UTP, pero el primero tiene un escudo metálico tejido que rodea los pares para que, de esta forma, se reduzca la probabilidad de que se presente interferencia proveniente de fuentes eléctricas fuera del cable.

El cable coaxial consiste en un conductor central de cobre envuelto con un material de plástico aislante que está, a su vez, cubierto por un tejido metálico y finalmente, por un forro de plástico. (El diseño del cable coaxial que se utiliza en las televisiones es similar). Se usan principalmente dos tipos en las redes. Thin Ethernet (10Base-2) utiliza cable RG-58/AU o RG-58/CU, mientras que Tick Ethernet (10Base-5) utiliza —usted lo adivinó— un cable mucho más delgado llamado RG-8. La figura 4-6 muestra un ejemplo de cable coaxial.

El cable de fibra óptica utiliza un filamento de vidrio que transporta las señales de datos como luz en lugar de electricidad. Antes era una costumbre utilizar el cable de fibra óptica en redes de alta velocidad, pero ahora está cambiando. Éstas son buenas noticias, ya que el cable de fibra óptica es extremadamente caro de comprar, instalar y proporcionar mantenimiento. Sin embargo, el cable de fibra óptica puede hacer una cosa que los cables de cobre no: conectar puntos extremadamente distantes pues, por ejemplo, puede cubrir dos millas a 100 Mbps, fácilmente. Por esta razón, a menudo se utiliza para conectar varios edificios para formar todo un campus. Sin embargo, exceptuando las situaciones en las que se necesite cubrir distancias muy grandes, usted debe evitar el uso del cable de fibra óptica.

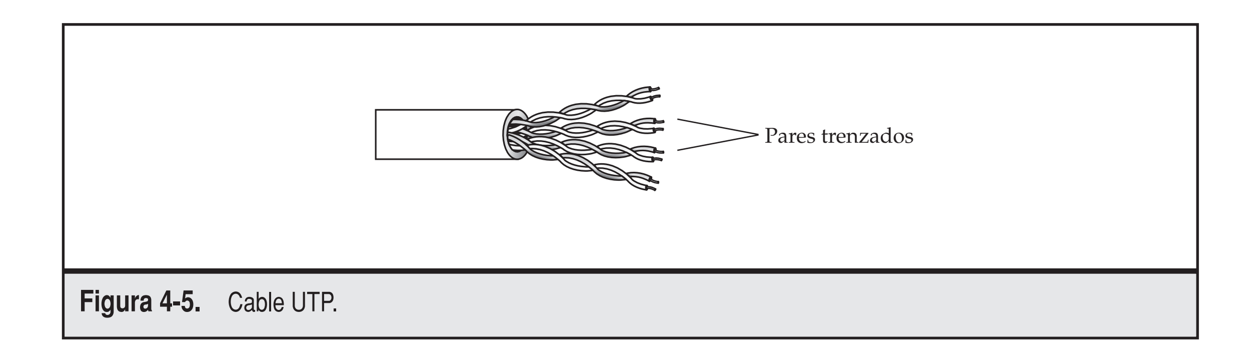


Figura 4-5. Cable UTP.

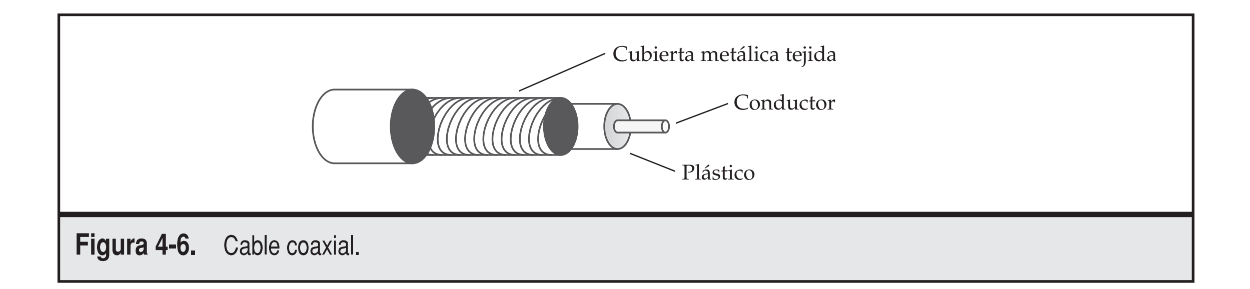


Figura 4-6. Cable coaxial.

Cableado con par trenzado: el rey de los cables de red

En los últimos años, virtualmente todas las redes se han instalado con el empleo de alguna forma de cable de par trenzado. Normalmente se ha utilizado el cable de par trenzado Cat-5, aunque existen muy pocas redes instaladas con cable Cat-3. El cable UTP se usa en lugar del STP la mayoría de las veces, debido a que es más barato, a la vez que es fácil de instalar y de dar mantenimiento y no es afectado por la interferencia eléctrica aun cuando no tenga forro. Tanto las redes

¿10Base qué?

Los diferentes estándares de Ethernet a los que se ha hecho referencia, por ejemplo, 10Base-2, 10Base-T, 100Base-T, etc., llevan implícitos en su nombre todo lo que necesita saber acerca de lo que hacen. La primera parte —el número— puede ser 10, 100 ó 1000, indica la velocidad de datos (en Mbps) que maneja el estándar. La palabra *base* significa que la red es *banda base*, en vez de *banda ancha*. (Una conexión banda base solo transporta una señal a la vez, mientras que una banda ancha transporta múltiples señales a la vez). La última letra o número indica qué tipo de cable utiliza, donde la T significa par trenzado; 2 representa coaxial delgado; 5 significa coaxial angosto y F o X, en general, indica cable de fibra óptica. Ésta es una referencia rápida a los estándares comúnmente encontrados:

- **10Base-2** 10 Mbps, cable coaxial (RG-58).
- **10Base-5** 10 Mbps, cable coaxial (RG-58).
- **10Base-T** 10 Mbps, cable de par trenzado (dos pares, Cat-3 o mayor).
- **100Base-T** 100 Mbps, cable de par trenzado (dos pares, Cat-5). También, existe una variante llamada 100Base-T4, que tiene cuatro cables.
- **100Base-TX** 100 Mbps, cable de par trenzado (dos pares, Cat-5).
- **100Base-FX** 100 Mbps, cable de fibra óptica.
- **1000Base-T** 1 Gbps, cable de par trenzado (cuatro pares, Cat-5).
- **10GBase-X** 10 Gbps, cable de fibra óptica.

Ethernet como las Token Ring utilizan cableado con par trenzado. Observe que las diferentes variedades de Ethernet requieren diferentes cables y que algunos estándares a velocidades más elevadas requieren STP.

Cuando se instala una red de par trenzado, un número de componentes de cableado forman la corrida completa desde la estación de trabajo hasta el concentrador. Como se muestra en la figura 4-7, el cableado comienza en el concentrador, donde un cable de parcheo (generalmente de 6 a 10 pies de longitud) se conecta a un puerto en el concentrador con un panel de parcheo, mediante un conector RJ-45 en cada extremo. En el otro lado del panel de parcheo, el cable de par trenzado está cableado de manera permanente a la conexión del panel de parcheo, y después va hasta una conexión de pared (en una oficina, por ejemplo) a la que también se encuentra conectado de manera permanente. La conexión de pared tiene un conector RJ-45 en su otro extremo, al cual se conecta otro cable de parcheo y después se conecta a la tarjeta de interfase de red de la computadora (NIC). La distancia del conector en el concentrador al conector en la NIC de la computadora no debe exceder una longitud de 100 metros.

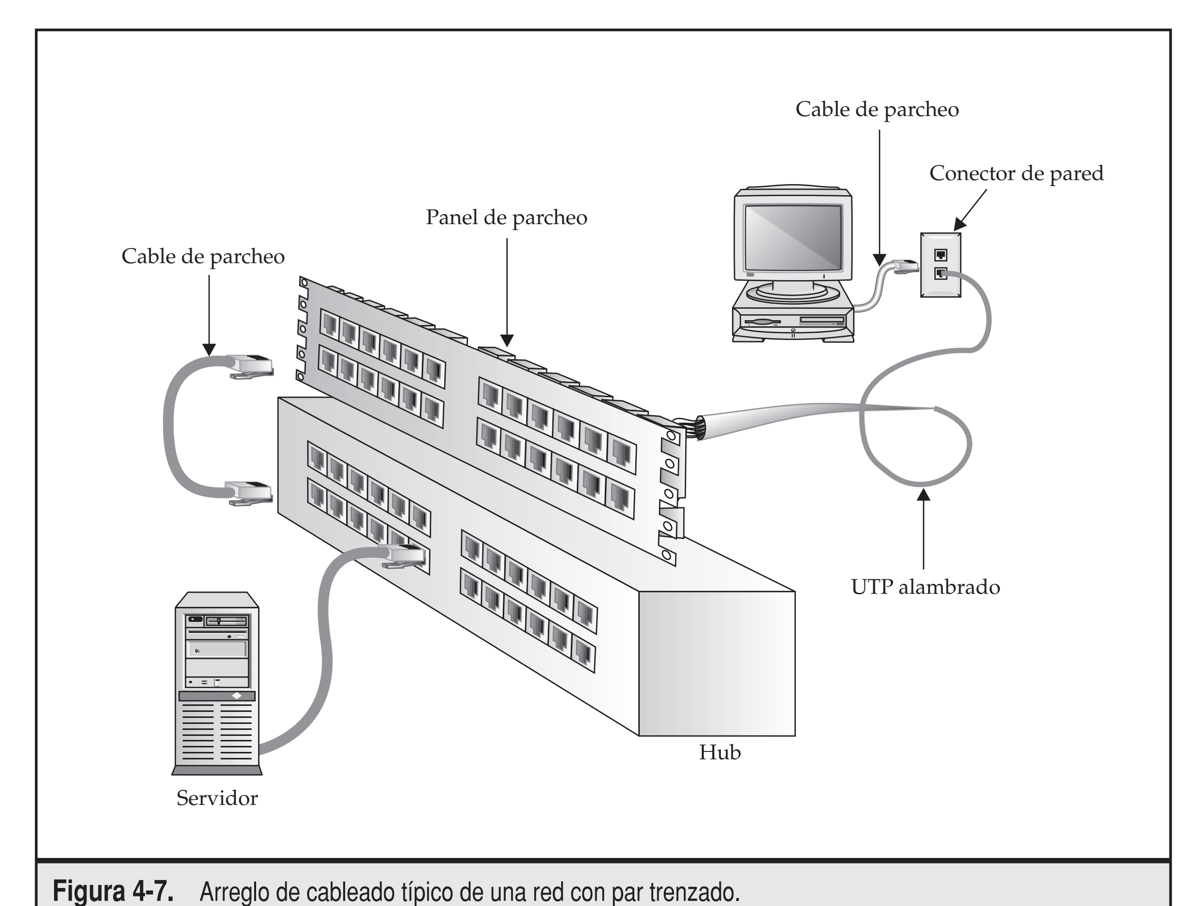


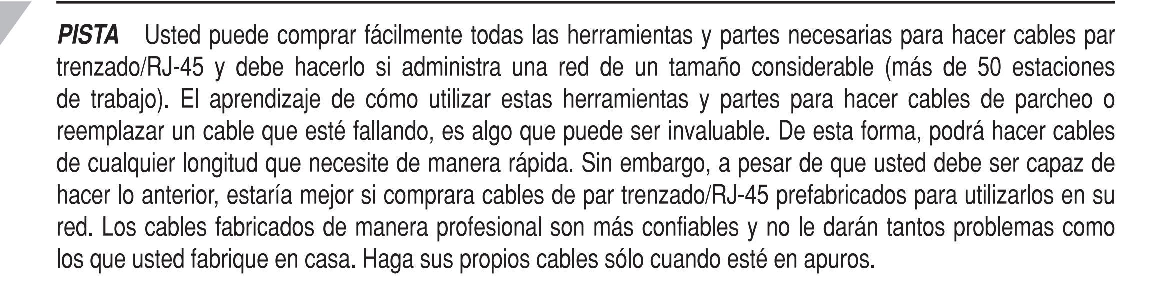
Figura 4-7. Arreglo de cableado típico de una red con par trenzado.

En cualquier punto donde el cable de par trenzado no esté conectado de forma permanente, se utilizan conectores modulares RJ-45. Éstos son idénticos a los conectores modulares que usted puede observar en los teléfonos, pero éstos son más grandes y tienen espacio para ocho alambres. Tanto 10Base-T como 100Base-T utilizan cuatro de estos alambres (dos pares: uno para transmitir y otro para recibir), mientras que 1 000Base-T utiliza ocho de estos alambres.

Los ocho alambres del conector RJ-45 están numerados del uno al ocho. Si fuera a sostener el conector en su mano izquierda con los pins del conector hacia arriba y hacia delante, el pin 1 del conector sería el más lejano a usted (vea la figura 4-8). La tabla 4-1 muestra los colores del cable estándar Cat-5 que deberá conectarse a cada pin y su uso en 10Base-T.

La mayoría de los dispositivos y redes de comunicaciones, incluyendo los diseñados para utilizar conectores RJ-45, son ya sea *equipo de comunicación de datos (DCE)* o *equipo terminal de datos (DTE)*. Si usted tiene equipo DTE en un extremo, necesita equipo DCE en el otro. De alguna manera, funciona como los tornillos y las tuercas. Dos tornillos no se colocan juntos con dos tuercas. El mismo principio se aplica aquí: el equipo DCE no puede hablar directamente con otro equipo DCE, ni un equipo DTE puede hablar directamente con otro equipo DTE.

El conector RJ-45 del concentrador es DCE, mientras que el conector RJ-45 de la tarjeta NIC de la computadora es DTE. Observe que no puede haber comunicación entre dispositivos DCE y DCE o entre DTE y DTE utilizando un cable de par trenzado/RJ-45 que se ha alambrado como se indica en la tabla 4-1. Por ejemplo, no puede utilizar un cable de parcheo estándar de par trenzado para conectar directamente un servidor de red con una estación de trabajo o entre dos estaciones de trabajo, ya que todos ellos son dispositivos DTE. En lugar de eso, debe comprar o armar un *cable de conexión* que compense tener, digamos, dos dispositivos DTE conectados directamente entre sí. La tabla 4-2 muestra al cableado necesario para armar un cable de conexión para redes 10Base-T.



PISTA Usted puede comprar fácilmente todas las herramientas y partes necesarias para hacer cables par trenzado/RJ-45 y debe hacerlo si administra una red de un tamaño considerable (más de 50 estaciones de trabajo). El aprendizaje de cómo utilizar estas herramientas y partes para hacer cables de parcheo o reemplazar un cable que esté fallando, es algo que puede ser invaluable. De esta forma, podrá hacer cables de cualquier longitud que necesite de manera rápida. Sin embargo, a pesar de que usted debe ser capaz de hacer lo anterior, estaría mejor si comprara cables de par trenzado/RJ-45 prefabricados para utilizarlos en su red. Los cables fabricados de manera profesional son más confiables y no le darán tantos problemas como los que usted fabrique en casa. Haga sus propios cables sólo cuando esté en apuros.

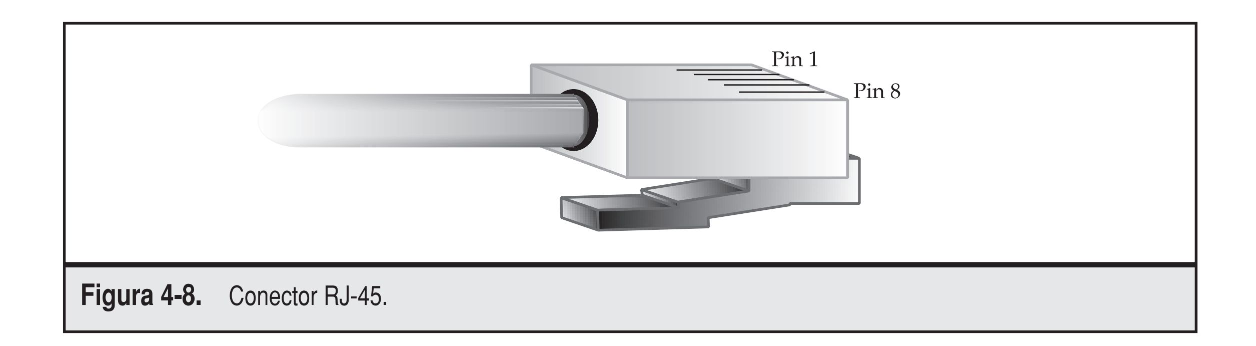


Figura 4-8. Conector RJ-45.

Número de pin	Color base del cable	Color de la cinta del cable	Uso del 10Base-T
1	Blanco	Naranja	Transmisión, negativo
2	Naranja	Blanco	Transmisión, positivo
3	Blanco	Verde	Recepción, negativo
4	Azul	Blanco	N/A
5	Blanco	Azul	N/A
6	Verde	Blanco	Recepción, positivo
7	Blanco	Café	N/A
8	Café	Blanco	N/A

Tabla 4-1. Asignaciones del cable 10Base-T para conectores RJ-45.

¿Qué significa todo eso acerca de las categorías de cable?

Los cables de red de par trenzado están categorizados de acuerdo con su capacidad para transportar tráfico a través de la red. Estas categorías se encuentran definidas por la Asociación de la Industria Electrónica (EIA) y se conocen como niveles 1 y 2 y categorías 3, 4, 5 y 6. Las diferentes categorías se llaman simplemente Cat-3 a Cat-6. La tabla 4-3 muestra el desempeño de cada nivel.

En la práctica, para lograr un desempeño en particular, no solo necesita un cable certificado con ese nivel de desempeño, sino que debe tener en cuenta otros requisitos, dentro de los que se incluyen el uso de conectores y cables de parcheo que también cumplan con el nivel de desempeño que usted desea alcanzar.

Extremo del cable 1			Extremo del cable 2		
Pin	Color base del cable	Color de la cinta del cable	Pin	Color base del cable	Color de la cinta del cable
1	Blanco	Naranja	1	Blanco	Verde
2	Naranja	Blanco	2	Verde	Blanco
3	Blanco	Verde	3	Blanco	Naranja
6	Verde	Blanco	6	Naranja	Blanco

Tabla 4-2. Cableado cruzado de par trenzado/RJ-45.

Nivel de categoría	Evaluación del desempeño
Nivel 1	Sin evaluación de desempeño
Nivel 2	1 Mbps
Categoría 3	10 Mbps
Categoría 4	16 Mbps
Categoría 5	100 Mbps to 1 Gbps
Categoría 6	>1 Gbps

Tabla 4-3. Designaciones de desempeño del par trenzado.

Por ejemplo, en una red que tenga Cat-5, usted debe utilizar cable, conectores, paneles y cables de parcheo Cat-5. Todo el circuito, desde donde la computadora del cliente se conecta hasta la conexión del concentrador en el otro extremo, necesita probarse y certificarse al nivel de desempeño que desee alcanzar.



PISTA Usted puede utilizar los sistemas de cable de mayor desempeño en redes que tengan requisitos bajos. Por ejemplo, es una práctica muy común en estos días emplear cable Cat-5 en todo el cableado de la red, aun si ésta solo utiliza 10Base-T a 10 Mbps. Hacer esto tiene sentido, ya que la planta de cable es muy costosa de reemplazar y utilizar cable Cat-5 significa que usted no tendrá que reemplazar el cableado de red cuando ésta se actualice a 100Base-T o algún estándar más elevado. Asimismo, los componentes del cableado con Cat-5 son de mayor calidad que los de Cat-3, por lo que es muy probable que su cableado de red sea más confiable. De manera similar, si cablea una red, deberá utilizar como mínimo Cat-5E o aun Cat-6, de forma que no tenga que reemplazar el cableado a medida que evolucione su red hacia estándares más novedosos.

Cable coaxial

Muchas redes anteriores (las diseñadas antes de 1992) se instalaron todavía con cable coaxial. La mayor parte de este cable es de tipo angosto, RG-58, y se utiliza con Thin Ethernet. Algunas pueden utilizar cable RG-8 angosto para Tick Ethernet, pero es raro.

El Thin Ethernet se cablea en una topología bus, donde cada segmento de red empieza con un terminador que se conecta al extremo del cable, se prolonga a cada nodo y finaliza con un terminador en el otro extremo. Los terminadores tienen resistencias especiales de 50 ohms y el cable de red no funcionará a menos que ambos se encuentren instalados.

Todos los conectores de un sistema Thin Ethernet son BNC, un conector tipo bayoneta fácil de liberar, tanto confiable como de fácil uso. Estos conectores se encuentran disponibles en una gran variedad de estilos para que usted pueda hacer cualquier conexión de red que necesite a lo largo del bus, incluyendo los conectores T, los cuales tienen dos conectores hembras tipo

Cable pleno contra cable no pleno

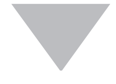
En un edificio, al área entre el techo de los cuartos y el techo del edificio se le llama *espacio pleno*. La mayor parte de los edificios utilizan ductos (mangueras grandes y flexibles) para proporcionar aire acondicionado a los cuartos, y éstos utilizan el espacio pleno abierto para el aire que regresa de los cuartos. Es típico que el aire que regresa de los cuartos sea reutilizado, de manera parcial, por las unidades de aire acondicionado a fin de ahorrar energía ya que se encuentra frío o caliente, según convenga, lo que significa un ahorro significativo de energía respecto al uso de todo el aire que viene del exterior. En ocasiones, los edificios utilizan ductos para el aire de retorno, pero lo normal para espacios con oficinas es utilizar simplemente el espacio pleno.

¿Por qué es importante este estudio acerca del manejo del aire en los edificios con oficinas en este capítulo? Porque para instalar el cable de red a través del techo de un edificio que utiliza el espacio pleno para el retorno de aire debe instalar el cable dentro de una tubería especial llamada *tubería de conduit* (la cual es extremadamente cara) o utilizar cable de tipo pleno. La diferencia entre cable no pleno y cable pleno es que el plástico que se utiliza en el cable pleno no libera gases tóxicos en caso de incendio. Debido a que en la mayoría de los edificios de oficinas se reutiliza el aire en el espacio pleno, la última cosa que los ocupantes desearían que pasara sería que los cables redistribuyeran gases tóxicos si se presentara un incendio en algún punto del techo del edificio o en el espacio pleno. Un incendio en un área muy pequeña podría provocar que los humos del cable incendiado se distribuyeran en un área muy grande del edificio debido a la forma en que funcionan estos sistemas de ventilación.

Asegúrese de verificar con su proveedor de cableado los detalles acerca de la zona donde esté instalado el cable de red, pero virtualmente todos los códigos de área en Estados Unidos requieren que los edificios con regreso de aire por el espacio pleno utilicen conduit o cable tipo pleno. Además de seleccionar el tipo de cable correcto, es también importante que el instalador esté familiarizado y a gusto con la realización de cualquier entrada en la pared que se requiera en corredores peligrosos o zonas de fuego del edificio. Dichas entradas en la pared deben sellarse adecuadamente para conservar los índices de fuego en el edificio.

BNC en cada lado del cruce de la T y un conector macho del mismo tipo en el extremo de la flecha de la T. Los dos conectores hembra se utilizan para el cable RG-58 que viene desde y hacia un nodo, mientras que el conector macho se conecta al conector BNC hembra de la tarjeta Ethernet del nodo. Existen también conectores tipo barril, los cuales tienen dos conectores hembra incluidos; éstos se utilizan para conectar dos cables Thin Ethernet. Los conectores tipo barril también se encuentran disponibles en formas diferentes, incluyendo en forma de codo o en forma de U, pero la mayoría de las veces se utiliza el conector recto tipo barril. La figura 4-2 que se mostró con anterioridad, presenta las diferentes partes de un sistema de cableado Thin Ethernet con BNC.

El cable coaxial tiene un *conductor* central, el cual puede ser un solo alambre sólido de cobre o un conjunto de alambres trenzados. Un material blanco de plástico rodea al conductor central, el cual, a su vez, está rodeado por una hoja metálica y por una *cubierta* de alambre tejida. La cubierta está, por último, envuelta en un forro de plástico.



PISTA En cualquier red de cable coaxial, los tipos de cable no deben combinarse. Si la red utiliza, digamos RG-58A/U, entonces ésos son los que usted siempre deberá usar, no cualquier otro cable coaxial. También es una idea no mezclar RG-58A/U y RG-58/U, ya que éstos tienen características de señalización diferentes. (El cable A/U utiliza un conductor central tejido, mientras que el /U —con frecuencia llamado C/U— utiliza un conductor central sólido).

Aprender a hacer cables coaxiales con conectores BNC es muy fácil, pero necesita dos herramientas especiales para que el trabajo sea más fácil. Primero, unas pinzas para cable a fin de cortar varios tramos de cable con la longitud correcta. Muchas pinzas pueden hacer esto por usted de manera automática; verifique con su proveedor de cable para solicitar una. Usted también necesitará una torcedora que tanto pueda torcer el pin BNC central en el conductor del cable, así como la manguita metálica que fija a todo el conector en el alambre. De nuevo, puede comprar torcedoras especiales que pueden hacer el trabajo más fácilmente. Las mejores torcedoras utilizan un mecanismo de rueda dentada con fiador a fin de ejercer, con mayor facilidad, la fuerza adecuada para realizar una conexión sólida y confiable.

INSTALACIÓN Y MANTENIMIENTO DEL CABLEADO DE LA RED

No solo es importante la selección del tipo de cableado de red, sino que también lo es instalar el cable correctamente. Una adecuada instalación de la planta de cableado deberá tener en cuenta los siguientes aspectos:

- Conectores y cable adecuados para el tipo de red, incluyendo la documentación acerca de los componentes que se seleccionaron y utilizaron. (Este requisito tiene por objetivo que el personal que, en el futuro, realice adiciones a la red pueda estar seguro de que está cumpliendo con dichas selecciones).
- Etiquetado de todas las partes de la red, incluyendo las conexiones de pared, los cables, los puertos del panel de parcheo, los cables de parcheo y las asignaciones de los puertos del concentrador. Este punto es importante para efectos de reparación.
- Un plano del edificio como *fue construido* en el que se muestren todas las rutas de cableado y ubicaciones.
- Un reporte de certificación que muestre que todos los cables instalados operan adecuadamente utilizando un dispositivo especial para la prueba de redes.
- En el caso de redes tipo bus, enseñar a los usuarios que no deben tocar el cable por ninguna razón. El cable coaxial provocará que todos los demás nodos en el segmento fallen si el cable es dañado. Asegúrese de que el personal de ese edificio también sepa todo ello.

Asegurarse de que la instalación de la planta de cableado está bien hecha y bien documentada le ahorrará tiempo a largo plazo, pues la red será más confiable y más fácil de reparar y dar mantenimiento.

Selección del proveedor del cableado

Cuando vaya a construir una nueva red, la selección de un proveedor de cableado es extremadamente importante. Un proveedor que haga un trabajo bien documentado y de alta calidad es muy deseable, pero es difícil de encontrar.

Cuando seleccione un proveedor, asegúrese de que él o ella tenga mucha experiencia en la instalación de redes como la que está instalando. Además, evalúe los aspectos siguientes como parte de su selección:

- ¿Cómo documentará el proveedor la planta de cableado? ¿Cuáles son sus estándares? ¿Cree que esos estándares de documentación cumplan con sus necesidades? (Recuerde, no existe mucha documentación acerca de plantas de cableado).
- ¿Entregará el proveedor un grupo de planos de la construcción del edificio que muestren cómo instaló los cables en el edificio?
- ¿Cómo instalará el proveedor el cable a fin de evitar fuentes de interferencia eléctrica en los techos y en las paredes?
- ¿Recomienda el proveedor una solución de cableado en la que se combinen los cables de telecomunicaciones con los de datos? (En general, mantener estas dos plantas separadas es lo mejor. Ambas tienen requerimientos diferentes y responden de manera distinta a las condiciones del edificio. Lo que funciona bien para los teléfonos puede que no funcione para el cableado de red y viceversa).
- ¿Qué equipo utiliza el proveedor para certificar la planta de cableado? ¿Qué documentación de certificación proporcionará una vez que haya terminado?
- ¿Ofrecerá el proveedor servicios de reparación de fallas después de la instalación?

Asegúrese de invertir el tiempo suficiente para buscar los mejores proveedores de cable disponibles y compárelos con mucho cuidado. Quizás usted quiera contactar otras compañías como la suya o grupos de usuarios de computadoras en su localidad, a fin de buscar recomendaciones y experiencias con los diferentes proveedores. Trate de no depender sólo de las referencias que le proporciona su proveedor; incluso las firmas que no hacen muy bien el trabajo pueden proporcionarle buenas referencias.



PISTA Para el caso de un trabajo de cableado grande, asegúrese de negociar un calendario de pagos adecuado. Usted debe tener la idea de pagar 30% del monto al inicio, 50% al término y 20% durante la entrega de los planos de cableado, reportes de certificación y cualquier otra entrega final. Prometa pagar una cantidad no menor a 15% en la entrega final a fin de asegurar que el proveedor de cable los entregue oportunamente. Los proveedores son famosos por fallar en este tipo de entregas una vez que ha sido terminada la instalación, por lo que necesita asegurarse de tener una forma de motivarlo para que termine todo el trabajo.

Resolución de los problemas de cableado

Los problemas de cableado pueden ser extremadamente difíciles de diagnosticar y reparar. Muchos son intermitentes o tienen como consecuencia la reducción del ancho de banda de los nodos afectados. El rastreo de la fuente del problema puede ser difícil. ¡A veces, es difícil saber siquiera si existe un problema!

Los problemas con el cableado de las redes se presentan de las siguientes formas:

- Desempeño de red demasiado pobre, en particular si un nodo es mucho más lento que otros nodos similares (en el caso de las redes en estrella), o si todos los nodos de un segmento tienen un desempeño menor que los nodos de otros segmentos (en el caso de las redes tipo bus).
- Desconexiones esporádicas de la red.
- Pérdida completa de conectividad de la red. Este problema puede ser intermitente.

Las redes tipo estrella son las más sencillas de reparar. Debido a que cada nodo está en su propio cable de red que lo conecta con el concentrador, es relativamente fácil aislar el problema. Si usted tiene dificultades con un nodo en una red topología estrella, primero determine si algo está mal en la computadora o el cableado. Mueva la computadora a un punto diferente en el edificio y observe si se presenta el mismo problema. En caso afirmativo, entonces es muy probable que el problema resida en la computadora y puede ser que la que falla sea la NIC. Segundo, si la computadora tiene un desempeño de red normal en un punto diferente, trate de reemplazar al cable de parcheo que va del nodo a la pared. A menudo, estos cables se dañan ligeramente por efecto del movimiento de los muebles y las computadoras de un lugar a otro. Enseguida, en el closet de cableado usted puede tratar de conectar el panel de parcheo de la ubicación del nodo a un puerto diferente en el concentrador, mediante un cable de parcheo diferente. Mientras que una falla en los paneles de parcheo en los closets de cableado es menos probable que se presente, debido a que éstos no tienen mucho movimiento, pueden tener conexiones o cableado muy pobres que, con el paso del tiempo, se conviertan en algo problemático. Por último, si ha eliminado todos los demás factores, debe considerar el reemplazo del cable que va desde el closet de cableado hasta la ubicación del nodo. En este punto, es muy recomendable contratar a un proveedor calificado de cableado para que lo ayude. Éste cuenta con el equipo necesario para probar el cable sobre la pared y determinar si está mal antes de instalar otro cable como reemplazo. Por la ayuda en la reparación, usted debe planear un pago de aproximadamente 150 dólares al proveedor que vaya a sus instalaciones y pruebe esta parte del cableado. Si por alguna razón tiene que instalar un cable nuevo en la parte afectada, tendrá que pagar la mano de obra y los materiales necesarios para realizar ese trabajo.

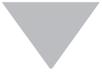
Las redes de cable coaxial pueden ser mucho más difíciles de reparar debido a que muchos nodos comparten un solo segmento de la red. A menudo, un problema en una parte del segmento afecta a todos los nodos del segmento de la misma forma. El problema muy usual en las redes de cable coaxial es la pérdida de la conectividad de red de todos los nodos del segmento. Alguna persona que desconecte el cable de red invariablemente provocará esta pérdida. Para rastrear este problema, 90% de las veces usted encontrará que será necesario encontrar quién movió o cambió el arreglo de las oficinas, o qué oficinas estaban siendo pintadas, o en qué parte otro trabajo de este tipo se estaba llevando a cabo en el edificio. Las probabilidades de que el problema se encuentre ahí son altas. Sino es así, entonces el trabajo de reparación se convierte

en algo mucho más complejo. Existen dos maneras de rastrear rupturas de cable que no son muy obvias:

- ▼ Utilice un explorador de cable coaxial. Estos instrumentos portátiles, que se conectan a un cable de red coaxial pueden proporcionarnos información sobre qué tan lejos del cable se ha presentado un corto o una ruptura. Continúe conectando el aparato al cable de red en diferentes puntos hasta que pueda detectar el problema.
- ▲ Obtenga un terminador extra para la red y después desconecte el cable en una ubicación en particular y conecte el terminador. Observe si las computadoras del segmento nuevo más pequeño pueden acceder al servidor. (Debe haber un servidor disponible en el mismo segmento; de otra forma, usted puede utilizar el comando PING —si utiliza el protocolo TCP/IP en sus computadoras— y trate de enviar un ping a otra estación de trabajo en el segmento). Si es así, entonces sabe que el problema se encuentra más adelante sobre el cable. Muévase a otro punto, conecte el terminador y trate de hacer lo mismo. En cualquier momento, usted encontrará dos puntos cercanos donde el terminador permitirá que la red trabaje en un punto pero no en el siguiente. Luego deberá encontrar el problema del cable en un punto entre esas dos ubicaciones. Este método requiere de paciencia, pero funciona bien para un caso de apuros.

Más engorroso es aún, en las redes de cable coaxial, un problema que sólo permita un desempeño muy pobre de la red, pero que no esté provocando que algún nodo la desconecte. Puede ser difícil encontrar este tipo de problemas, ya que a menudo son intermitentes y no es sencillo detectarlos con el aparato explorador. Cuando usted tenga este tipo de problema, el mejor método es realizar una prueba de la cual se pueda determinar rápidamente qué tan rápido se comunican los nodos con la red. Por ejemplo, puede medir el tiempo que toma copiar un archivo determinado al servidor. Después, utilice un terminador para asilar una parte del segmento y llevar a cabo la prueba otra vez. Continúe moviendo el terminador y repitiendo la prueba hasta que descubra qué parte del cable hace más lento el desempeño de la red en el segmento. Después, reemplace todas esas porciones o reduzca un poco más su búsqueda. Este tipo de problemas son generalmente causados por una conexión pobre en uno de los conectores macho BNC, aunque un conector tipo barril o tipo T que esté suelto también puede causarlo. En general es más rápido, —a menos que usted reduzca el problema a un área lo suficientemente pequeña— simplemente reemplazar todo el cable y los conectores en ese punto.

Contar con una segunda persona que ayude a reparar los problemas de cable coaxial ayuda mucho y se puede encontrar el problema más rápidamente si usted y los demás reparadores cuentan con radios portátiles (o teléfonos celulares) con los cuales comunicarse. Una forma de aprovechar este procedimiento consiste en asignar a una persona en un extremo del segmento con una computadora de prueba y, después, hacer que la otra persona se mueva de lugar en lugar con un terminador. Mientras el reparador móvil realiza pruebas de partes del segmento con el terminador, la persona estacionaria realiza pruebas rápidamente para ver si alguna parte del segmento es la fuente del problema.



PISTA Antes de meterse en el problema de jalar una nueva sección de cable a través de la pared o reemplazar varios cables y conectores, trate simplemente de instalar un cable extra de un punto a otro, como fuera de la puerta de un cuarto, a lo largo del pasillo y dentro de otro cuarto. Después, pruebe para ver si este "mapeo" de la porción del segmento bajo sospecha elimina el problema. Si el problema queda resuelto, siga adelante e instale un nuevo cable en las paredes. Si el problema persiste, necesita buscar más a fondo antes de reemplazar el cable y los conectores.

Como una regla general, la reparación de problemas en el cableado requiere un método paso a paso muy meticuloso y mucha paciencia. En los sistemas de cable coaxial, la reparación se torna más complicada, ya que muchos usuarios de redes lo estarán presionando muy fuerte mientras trata de concentrarse en la búsqueda del problema. Será muy afortunado si pudiera encontrar un problema en una red de cable coaxial y resolverlo en un periodo de una hora. Algunos problemas, sin embargo, pueden tomar algunas horas (o más) para resolverse.

RESUMEN DEL CAPÍTULO

En este capítulo usted aprendió acerca de los sistemas de cableado de las redes. Además, conoció las principales topologías con las que se cablean, cómo funcionan las redes CSMA/CD y de estafeta circulante, qué tipos de cable se utilizan comúnmente y cómo deben instalarse. También recibió algunos consejos respecto a la selección del proveedor de cableado y a la reparación de los problemas en el cableado de red.

El capítulo siguiente abunda sobre este análisis y se enfoca en la creación de redes para la oficina doméstica o pequeñas oficinas y, como parte de este análisis, aprenderá también acerca de la conectividad inalámbrica.

CAPÍTULO 5

Conectividad de redes domésticas

Mientras que éste es un libro cuyo enfoque es la conectividad de redes de negocios, la conectividad de oficinas pequeñas y domésticas (SOHO) está creciendo en importancia, por lo cual ningún estudio sobre el tema estaría completo si no se ofreciera un panorama sobre conectividad doméstica. Debido a que es cada vez más común en estos días que las familias adquieran e instalen múltiples computadoras en sus hogares, es importante que usted conozca este tipo de conectividad.

BENEFICIOS DE LA CONECTIVIDAD DE REDES DOMÉSTICAS

Muchos de los beneficios que reporta a los negocios tener una red, también se aplican a los hogares que tienen múltiples computadoras. Considere:

- Las impresoras pueden compartirse, lo cual permite que todos los usuarios de computadoras del hogar puedan usar todas las impresoras. Por ejemplo, algunas casas pueden tener impresoras láser blanco y negro e impresoras de inyección de tinta a color. Compartirlas por medio de una red doméstica permite a cada persona utilizar la impresora más adecuada para cualquier trabajo que deba realizar.
- Se puede compartir una conexión de Internet de alta velocidad. En muchos lugares existen diferentes conexiones de este tipo que incluyen DSL y redes por cable. Ambos tipos de redes pueden configurarse para soportar múltiples computadoras en casa. Sin embargo, con la finalidad de aprovechar dichas conexiones, las computadoras deben formar parte de una red dentro de casa.
- Pueden compartirse los archivos y el espacio disponible en disco puede utilizarse de una manera más eficiente. A veces, a una computadora se le puede terminar el espacio para almacenamiento. Sin embargo, en una red doméstica, todas las computadoras de la casa pueden utilizar el espacio disponible en todas las demás computadoras, lo cual significa ahorrar dinero que, de otra forma, sería necesario gastar en la compra de más computadoras o discos duros adicionales. Por ejemplo, algunos archivos podrían moverse de una computadora a otra y después, la computadora original podría accesarlos a través de la red.
- Los dispositivos de respaldo también pueden compartirse. En una red doméstica, los archivos críticos de todas las computadoras pueden respaldarse, mediante el uso de la red, en un dispositivo controlador de cinta, o CD o quemador DVD. Asimismo, los archivos críticos de cada sistema pueden ser copiados en el otro a fin de hacer un respaldo, siempre y cuando las computadoras cuenten con el espacio libre suficiente para permitir este arreglo.
- Si usted va a instalar una red doméstica inalámbrica, podrá acceder de una manera más conveniente a Internet y a otros recursos de la red doméstica desde una computadora portátil en cualquier punto de la casa o, incluso, desde fuera de ésta.

Estoy seguro de que usted puede ver cómo estos beneficios pueden ser de utilidad en los hogares que tienen más de una computadora. La pregunta que sigue es, ¿cuál es la mejor forma de seleccionar e instalar una red doméstica?

SELECCIÓN DE UNA TECNOLOGÍA PARA UNA RED DOMÉSTICA

Debido al crecimiento del interés en la conectividad de redes domésticas, en la actualidad muchos fabricantes ofrecen hardware y software especial para este tipo de conectividad. Además, en muchos casos, una red doméstica puede aprovechar el hardware y software tradicional para conectividad de redes. Esta sección proporciona un panorama de las diferentes opciones de conectividad de redes domésticas.

Hardware estándar de red

En realidad, antes no era factible que las redes domésticas utilizaran equipo para la conectividad de redes diseñado para los negocios, ya que éste era muy costoso y estaba pensado solo para soportar grandes redes. ¡Un concentrador Ethernet de 24 puertos definitivamente estaría subutilizado en una casa con dos o tres computadoras!

Sin embargo, en estos días el equipo para redes de negocios se encuentra disponible en todas los tamaños y formas, y las soluciones que se diseñaron para los negocios a menudo funcionan muy bien en la mayoría de los hogares. Los concentradores y switches Ethernet pequeños que pueden soportar de dos a cuatro computadoras, de forma económica, se encuentran disponibles en el mercado desde 50 a 75 dólares aproximadamente.

Si usted considera todos los componentes que necesitaría para una red pequeña, encontrará que, en realidad, no necesita tanto dinero:

- Un concentrador o switch central. Puede instalarlo en un punto conveniente, como donde se ubica el cableado telefónico de la casa o en el lugar de estacionamiento, en el closet, en el desván o en el sótano. Asimismo, necesitará un contacto de alimentación de energía eléctrica para alimentar el concentrador en dondequiera que éste se encuentre ubicado.
- Cada computadora necesita una tarjeta de interfase de red (NIC) que soporte el tipo de red que quiera instalar. La mayoría de las computadoras modernas vienen con tarjetas Ethernet 10/100/1000 Base-T instaladas dentro de las mismas. Si la suya no tiene una de estas tarjetas, es fácil y barato comprar e instalar un estándar NIC en la mayoría de las computadoras. El costo de una NIC de Ethernet es de menos de 50 dólares. Asimismo, existen buenas interfases de Ethernet que pueden conectarse a un puerto USB de computadora, y éstas tampoco son muy costosas y trabajan muy bien.
- Usted necesitará cablear la red. Esto, en realidad, es la parte más difícil, pues depende de la ubicación real de las computadoras y la facilidad con la que pueda llevar el cable de red a cualquier lugar donde se necesite. Si no desea instalar este cable usted mismo, un buen electricista o técnico en cableado telefónico podría hacer un buen trabajo por usted. El costo del cableado profesional es de 100 a 150 dólares aproximadamente por corrida de cable, lo cual incluye la instalación de todos los conectores, el cable y elementos adicionales como las placas de pared y los dispositivos de enchufe.
- El sistema operativo de la mayoría de las computadoras domésticas —generalmente Windows XP, sin embargo, en algunos casos Windows 9X o Windows Me— puede manejar perfectamente todas las tareas de conectividad de redes que usted necesitará para una red doméstica. Si usted configura los sistemas operativos en una red de igual

a igual, podrá compartir impresoras y archivos por medio del software de conectividad de redes instalado en el sistema. No se necesita software adicional.

Todos estos componentes se encuentran disponibles de manera separada, como lo compraría para un negocio. Sin embargo, existen kits de conectividad de redes domésticas que incluyen todos los componentes que usted necesita, junto con instrucciones para la configuración de su red.



PISTA Un libro como éste no puede hacer recomendaciones detalladas acerca de un producto, en parte porque los productos y la tecnología cambian más rápido que los libros. Es una buena idea, por tanto, buscar información reciente de productos para la conectividad de redes domésticas y utilizarla para decidir qué productos adquirir. Hay revistas muy buenas que tienen información de productos muy novedosos, incluyendo análisis de algunos caseros. Verifique su biblioteca o el estante de revistas en su librería local.

Inalámbrica u otras opciones de conectividad de redes

Vale la pena repetir un aspecto de la sección anterior: la parte más difícil de la instalación de una red doméstica es el cableado. La mayoría de la gente no está calificada para instalar el cableado de la red, ni desea comenzar a hacer agujeros en sus paredes y tratar de adivinar cómo instalarlo por toda su casa (o bajo la misma). Debido a que ésta es la dificultad más grande en la instalación de una red casera, muchas compañías han inventado otras opciones de red que eliminan este problema, como las que se describen a continuación:

- **Redes que utilizan la línea telefónica** En la actualidad, se encuentran disponibles kits de redes caseras que utilizan el cableado telefónico existente a fin de ofrecer una conexión de red entre las computadoras de una casa. Esta opción se torna atractiva si existen conexiones telefónicas cerca de cada computadora. Intel, 3Com, D-Link y otras compañías ofrecen estos paquetes. Un recurso disponible en Internet para la conectividad de redes es **http://www.homepna.com**.
- **Redes que utilizan las líneas de alimentación eléctrica** Algunas compañías ofrecen hardware que le permite conectar computadoras utilizando el cableado eléctrico existente en su casa. El equipo de red transmite su información a través del cableado eléctrico, y todo lo que usted necesita hacer es conectar un adaptador especial en un contacto disponible que se encuentre cerca de la computadora. Las redes que utilizan los cables de alimentación eléctrica son más lentas que otros tipos de redes (la mayoría posee velocidades de aproximadamente 1 Mbps), y están sujetas al ruido eléctrico proveniente de diferentes tipos de equipos caseros. (En realidad, a una persona le fallaba la red de energía eléctrica de su casa cada vez que el compresor del refrigerador se encendía). Usted debe seleccionar una red con alimentación eléctrica solo como último recurso. Puede aprender más acerca de este tipo de redes en **http://www.homeplug.com**.
- **Redes inalámbricas** Definitivamente, la opción más popular en estos días es instalar una red inalámbrica en casa. Un gran número de compañías, entre ellas NETGEAR, D-Link y Linksys, ofrecen equipo inalámbrico para la conectividad de redes caseras. Estas redes, cuando utilizan la tecnología más actual, operan a una velocidad muy elevada: comienzan a 11 Mbps y muchas variantes van hasta los 54 Mbps; aun 11 Mbps debe ser más que suficiente para uso doméstico. Si usted decide hacer la prueba con

una red casera inalámbrica, debe estar consciente de que diferentes factores de su hogar (por ejemplo, la interferencia eléctrica de algunos aparatos eléctricos, o algo en las paredes que limite la conexión entre los cuartos o pisos) puede limitar la velocidad y la funcionalidad de estas redes. Por tanto, asegúrese de que pueda regresar o cambiar el equipo si no funciona adecuadamente en su casa.

Las soluciones inalámbricas han adquirido gran popularidad en los años pasados y se han logrado muchos desarrollos en esta área tecnológica. Existen tres estándares básicos inalámbricos que se emplean ampliamente: 802.11b, 802.11a y 802.11g. Es un poco contradictorio, pero en este caso, 802.11a es un estándar más rápido y avanzado que el 802.11b. El 802.11g es, en esencia, una mejora del 802.11b y utiliza las mismas frecuencias para transmitir datos. El 802.11g es líder en el mercado en la actualidad y existen muchas soluciones excelentes y relativamente baratas disponibles que utilizan este estándar, que incluyen algunas unidades de combinación de un punto de acceso inalámbrico 802.11g (también llamado WAP, un tipo de concentrador inalámbrico), con un ruteador diseñado para compartir una conexión a Internet casera de elevado ancho de banda entre múltiples computadoras. El gran atractivo de las unidades de combinación es que uno no necesita pagar más por el servicio de Internet de múltiples computadoras; el ruteador hace parecer como si sólo una computadora estuviera conectada a la red.

Descripción de una red inalámbrica

Existen algunos aspectos acerca de la tecnología inalámbrica que usted debería saber. El primero es que los estándares predominantes operan a velocidades de datos diferentes. El 802.11b opera a 11 Mbps, mientras que el 802.11g y 802.11a operan a una velocidad de hasta 54 Mbps. El segundo es que las particularidades de la casa y de otro equipo instalado pueden interferir con una red inalámbrica. Esto es más pronunciado con 802.11b y 802.11g, pues ambos operan a 2.4 GHz, la misma frecuencia a la que lo hacen muchos teléfonos portátiles y también cerca de la frecuencia de los hornos de microondas. (En realidad, hace varios años traté de instalar una red 802.11a en mi casa, y mientras que fue fácil de configurar y conectar, muchas conexiones fallaron y no pude usar mi teléfono portátil en ningún punto cerca de las conexiones de red inalámbrica debido a que producían interferencias audibles. El estándar 802.11a opera a 5 GHz, la cual es una frecuencia que está menos sujeta a la interferencia en una determinada casa). Tercero, una red inalámbrica lo expone a problemas de seguridad. Existen historias de mucha gente que se mueve en auto con computadoras portátiles y tarjetas de red inalámbricas instaladas tratando de encontrar una conexión disponible. Debido a que la mayoría de estos dispositivos trabajan en rangos mayores a 91.44 metros, usted debe preocuparse respecto a esta posibilidad. Es muy probable que sus vecinos "consigan un aventón" en su conexión a Internet a través de su red casera si no la asegura cuando la está instalando. Esto es más común de lo que piensa. Cuarto, esta área evoluciona a pasos agigantados, por lo que una solución que se adquiere hoy puede no ser compatible con el hardware equivalente que estará disponible en un par de años.

RESUMEN DEL CAPÍTULO

En este capítulo usted aprendió un poco acerca de la conectividad de redes caseras, un campo que actualmente cambia con mucha rapidez. En muchos casos, puede instalar una red casera utilizando componentes baratos disponibles en el mercado, diseñados para redes de negocios

pequeñas. El problema principal de esta opción reside en el cableado de la casa, aunque si todas las computadoras se encuentran en un solo cuarto, ello no representará mucho problema. En el caso de configuraciones más complejas o de querer tener más flexibilidad, aprendió acerca de tecnologías alternativas de conectividad de redes, incluyendo el equipo inalámbrico de conectividad para redes caseras.

En general, la mayoría de la gente debe investigar primero el equipo inalámbrico de conectividad para redes caseras. Actualmente este equipo trabaja bien en muchas casas, es barato y tiene buen soporte para este propósito. En algunos casos puede ser aceptable instalar equipo estándar de conectividad para redes cableadas o aun equipo de conectividad para redes que utilicen línea telefónica o cables de alimentación de energía eléctrica. Como siempre, analice sus propias necesidades con mucho cuidado y asegúrese de que pueda cambiar o devolver cualquier equipo de red casera si éste no funciona de manera adecuada en su casa.

CAPÍTULO 6

Comprensión del hardware de las redes

Si el cableado constituye el sistema nervioso de una red, entonces los dispositivos que se estudian en este capítulo representan los diferentes órganos. Los dispositivos de red estudiados en este capítulo —que incluye los repetidores, ruteadores, concentradores y por el estilo— son responsables de la transferencia de datos de un cable de la red a otro. Cada dispositivo tiene propiedades y usos diferentes. Un buen diseño de red utiliza el dispositivo correcto para cada tarea que la red debe cumplir.

En este capítulo aprenderá acerca del hardware esencial para la conectividad de redes, lo cual implica lo siguiente:

- Repetidores
- Hubs y concentradores
- Switches
- Puentes
- Ruteadores
- Compuertas
- Paredes
- Módems de corto alcance para conexiones pequeñas entre edificios

Es importante que entienda los componentes básicos que deben incluirse en la construcción de una red, así como el trabajo que cada persona realizará.

DIRIGIENDO EL TRÁFICO DE LA RED

La prueba crítica en cualquier diseño de red es su capacidad de dirigir el tráfico de un nodo a otro. Usted debe conectar los diferentes dispositivos de la red en una configuración que permita que la red transfiera las señales entre los edificios de una manera lo más eficiente posible, tomando en cuenta el tipo de red y los diferentes requerimientos de conectividad de ella. De entre los dispositivos básicos que puede utilizar para llevar a cabo lo anterior, se encuentran:

- **Repetidores**, los cuales extienden la distancia que el tráfico de red puede transferirse en un tipo de medio de transmisión en particular.
- **Hubs** (concentradores), los cuales se utilizan para conectar nodos entre sí cuando utiliza una topología estrella, como 100Base-T.
- **Puentes**, los cuales son, en esencia, repetidores inteligentes que envían el tráfico de un segmento a otro sólo cuando éste está destinado al otro segmento.
- **Ruteadores**, los cuales pueden enrutar, de manera inteligente, el tráfico de la red de muchas maneras.
- **Switches**, los cuales forman conexiones rápidas punto a punto para todos los dispositivos conectados a ellos. Las conexiones de un puerto a otro del switch se llevan a cabo conforme se necesiten y no se envían a los puertos que no estén involucrados en el tráfico. Debido a que limitan las conexiones realizadas, los switches pueden ayudar a eliminar las colisiones de tráfico provocadas por los segmentos que no se comuniquen.

Conectar todos los componentes necesarios en la forma correcta es el arte del diseño de las redes. En el capítulo 15 se estudian los aspectos importantes de la conexión de estas piezas de forma que trabajen de una manera óptima; sin embargo, usted primero debe conocer cuáles son estos dispositivos y qué pueden hacer. En las secciones siguientes se estudian.

Repetidores

Un *repetidor* es un dispositivo que extiende la distancia de un tramo de red en particular. Un repetidor toma una señal débil por un lado, la amplifica y, después, la manda por el otro lado. A menudo usted puede ver repetidores en las redes Thin Ethernet, pero se encuentran virtualmente en cualquier conexión de red. Por ejemplo, si tiene que instalar un tramo de cable Cat-5 100Base-T que sea mayor de 100 metros, un repetidor le permitirá duplicar esa distancia.

Los repetidores operan a nivel capa física del modelo OSI de conectividad de redes. Sin embargo, no poseen la inteligencia para comprender las señales que transmiten. Los repetidores sólo amplifican la señal entrante de cualquier lado y la repiten por el otro lado. (Sin embargo, ¡recuerde que también amplifican cualquier ruido que se produzca en el cable!). Los repetidores se utilizan para conectar solamente el mismo tipo de medio de transmisión, como de 10Base-2 Thin Ethernet a 10Base-2 Rhin Ethernet, o Token Ring de par trenzado con Token Ring de par trenzado.

Los repetidores poseen una pequeña cantidad de inteligencia que puede ser de utilidad. Pueden aislar una de sus conexiones de la otra cuando se presenta un problema. Por ejemplo, considere dos segmentos de Thin Ethernet que se encuentren conectados mediante un repetidor. Si uno de esos segmentos se rompe, el repetidor aún permite que el segmento que está en buenas condiciones continúe operando correctamente. Los usuarios de este segmento no podrán tener acceso a los recursos que se encuentran en el segmento roto, pero podrán continuar utilizando el segmento en buenas condiciones sin problema. (¡Recuerde, sin embargo, que esta capacidad no resulta del todo útil si sus servidores se encuentran en el lado roto y sus estaciones de trabajo están ubicadas en el segmento que no está roto!). La figura 6-1 muestra una extensión de red que utiliza repetidores.



PISTA Los repetidores, en general, se utilizan en redes 10Base-2 (Thin Ethernet), las cuales se estudiaron con más detalle en el capítulo 4.

Hubs y concentradores

Los *concentradores LAN inteligentes* —llamados de una manera más simple *concentradores* o, aún más simple, *hubs*— se utilizan para conectar los nodos de red a la columna dorsal de la misma. Los nodos se conectan a los hubs físicamente en forma de estrella (los cables se extienden desde el concentrador a cada nodo), ya sea que se utilicen en una red con topología estrella o con topología anillo. (Una red sencilla podría constar de uno o dos concentradores; redes más pequeñas generalmente no requieren una red de espina dorsal).

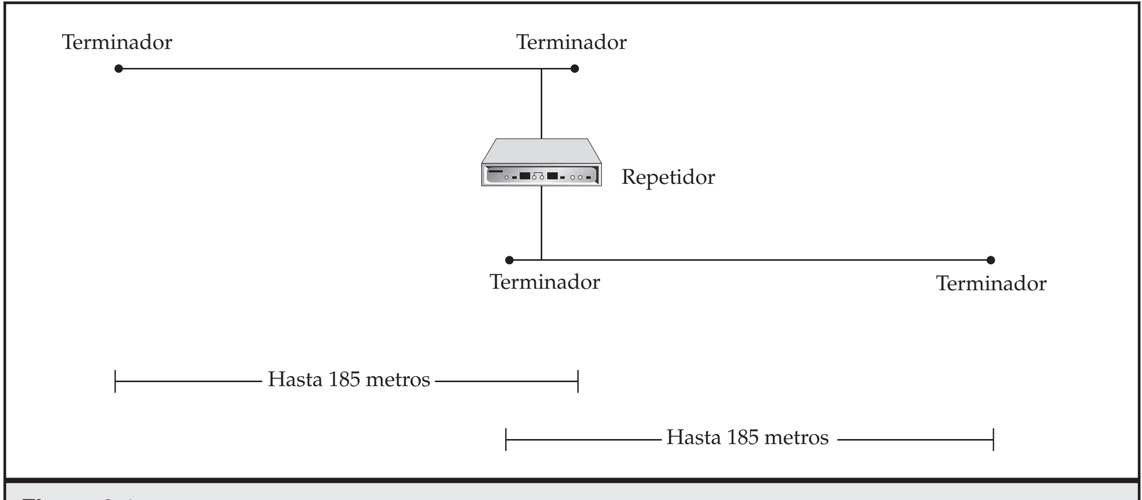


Figura 6-1. Utilización de repetidores para extender la longitud de la red.

NOTA El capítulo 4 presenta un estudio detallado de las topologías tipo bus, anillo y estrella.

Los hubs se encuentran disponibles para cualquier tipo de medio de transmisión que utilice módulos reemplazables para soportar diferentes tipos de medios de transmisión. Por ejemplo, puede comprar un chasis (bastidor) de concentrador en el que se puedan colocar tanto módulos Ethernet como Token Ring.

Usted puede comprar hubs en una gran variedad de tamaños que van desde los que soportan solo dos estaciones de trabajo hasta los que soportan más de 100 estaciones. Muchos diseñadores de redes utilizan hubs apilables, los cuales, en general, soportan 24 conexiones de nodo cada una. A menudo, estos hubs se utilizan en conjunto con switches, los cuales se estudian en una sección independiente en este capítulo.

Los hubs tienen dos propiedades importantes. La primera es que repiten todos los datos de cada puerto a todos los demás. Aunque están cableados en forma de estrella, en realidad trabajan eléctricamente (lógicamente) como si fuera un segmento con topología bus. Debido a esta repetición, no se presenta ningún filtrado o cualquier otra lógica para evitar las colisiones entre los paquetes que son transmitidos por cualquiera de los nodos conectados. La segunda propiedad importante que tienen los hubs es la *partición automática*, donde el hub puede automáticamente *partir* (en este contexto, cortar) cualquier nodo que tenga problema con los demás, desconectándolo. Dicha partición ocurre, por ejemplo, si se detecta un corto en el cable, si el puerto del hub recibe una cantidad excesiva de paquetes que inundan la red o si algún otro problema serio se detecta en un puerto determinado del concentrador. La partición automática previene que una conexión que no funcione de manera correcta provoque problemas a todas las demás.

A medida que transcurre el tiempo, los concentradores incrementan su nivel de complejidad. A menudo poseen una serie de características integradas avanzadas, dentro de las que se incluyen las siguientes:

- Administración integrada, que permite que el hub puede administrarse desde un punto central de la red mediante el empleo de SNMP u otros protocolos y software de administración de redes.
- Autodetección de diferentes velocidades de conexión. Por ejemplo, son comunes los concentradores Ethernet que puedan detectar y operar, de forma automática, cada nodo a 10 Mbps (10Base-T) o 100 Mbps (100Base-T).
- Enlaces de alta velocidad que conectan el hub a una espina dorsal. Éstas, en general, operan a 10 veces la velocidad nominal del hub. (Por ejemplo, para un concentrador de 100 Mbps, los puertos de enlace deben operar a 1 Gbps).
- Funciones integradas de puenteo y enrutamiento, las cuales hacen innecesaria la utilización de dispositivos separados para llevar a cabo el puenteo y el enrutamiento.
- Conmutación integrada que permite que los nodos del hub pueden conmutarse en vez de compartirse.

Cuando compre un concentrador, es importante saber cuántos nodos desea conectar, qué cantidad de ancho de banda requiere cada uno y qué tipo de bus de red se utilizará. Los buses pueden ser cualquiera, desde un bus Thin Ethernet a 10 Mbps, un bus 100Base-TX a 100 Mbps, hasta buses a más alta velocidad. Su selección en cuanto a una determinada tecnología de bus depende de la cantidad total de ancho de banda que usted necesite y de los demás criterios de diseño de redes con los que deba cumplir.

Cada concentrador tiene un *dominio de colisión* separado o área de la red en la que pueden presentarse colisiones. En general, conectar todos los hubs en alguna forma resulta en un dominio de colisión más grande, que abarca todos los hubs. La excepción a esta regla es una configuración donde todos los diferentes hubs se conectan a un switch (consulte la siguiente sección), el cual mantiene a cada hub en su propio dominio de colisión. La figura 6-2 muestra un ejemplo de una red que utiliza hubs.

Switches

Los *switches*, como su nombre lo indica, pueden conmutar conexiones de un puerto a otro y lo pueden hacer de manera muy rápida. Están orientados a la conexión y, de forma dinámica, conmutan entre sus diferentes puertos para crear estas conexiones. Piense en un patio de ferrocarril con muchos trenes acercándose en algunas vías y alejándose en otras, y que el switch es el administrador del patio y quien ordena que la vía "se conmute", de forma que los trenes lleguen a su destino. Un switch de red es muy parecido a este tipo de administrador, excepto que el switch dirige paquetes en lugar de trenes y utiliza cableado tipo Ethernet en vez de rieles de ferrocarril para transportar la mercancía.



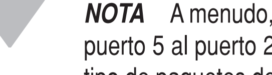
NOTA Los switches se parecen mucho a los puentes, excepto que los primeros tienen muchos puertos y de otra forma se verían como hubs. Usted debe pensar en un switch como un puente con múltiples puertos.

Debido a que los switches forman conexiones uno a uno entre cualquier par de puertos, todos los puertos que ingresan a un switch no son parte de un solo dominio de colisión. En este sentido, el switch actúa como un tipo de puente gigante. A menudo los switches se utilizan para conectar un número determinado de hubs a un bus más rápido. Por ejemplo, suponga

Cable
de bus
común

Figura 6-2. Arreglo típico de hubs.

que usted tiene 10 hubs, cada uno con 24 estaciones de trabajo conectadas. Si simplemente conecta todos los hubs en un bus común, las 240 estaciones de trabajo compartirían un único dominio de colisión, lo cual podría afectar un poco el desempeño de la red. En lugar de hacer eso, una forma mucho mejor es instalar un switch de 12 puertos y conectar cada hub a uno de los puertos del switch. Por ejemplo, es común utilizar 100Base-T Ethernet en las conexiones de las estaciones de trabajo, pero 1 000Base-T (o algún otra conexión de red más rápida) para el bus. Este arreglo, además, permite que todo el tráfico que se genere en cada uno de los 10 hubs continúe operando a una velocidad de conexión de red de aproximadamente 10 Mbps hacia los servidores, a pesar de que todos los hubs estén compartiendo el bus. La figura 6-3 ilustra este método.



NOTA A menudo, los switches se utilizan simplemente para conectar dos puertos dados (como el tráfico del puerto 5 al puerto 21, por ejemplo), pero también son lo suficientemente inteligentes como para repetir cierto tipo de paquetes de difusión a todos los puertos de forma simultánea.

Los switches se han abaratado mucho y son extremadamente rápidos. En las conexiones en redes de área local, el uso de switches tiene más sentido que el de ruteadores, parcialmente debido a su costo y su relativa simplicidad. En realidad, la adquisición de puentes se ha dificul-

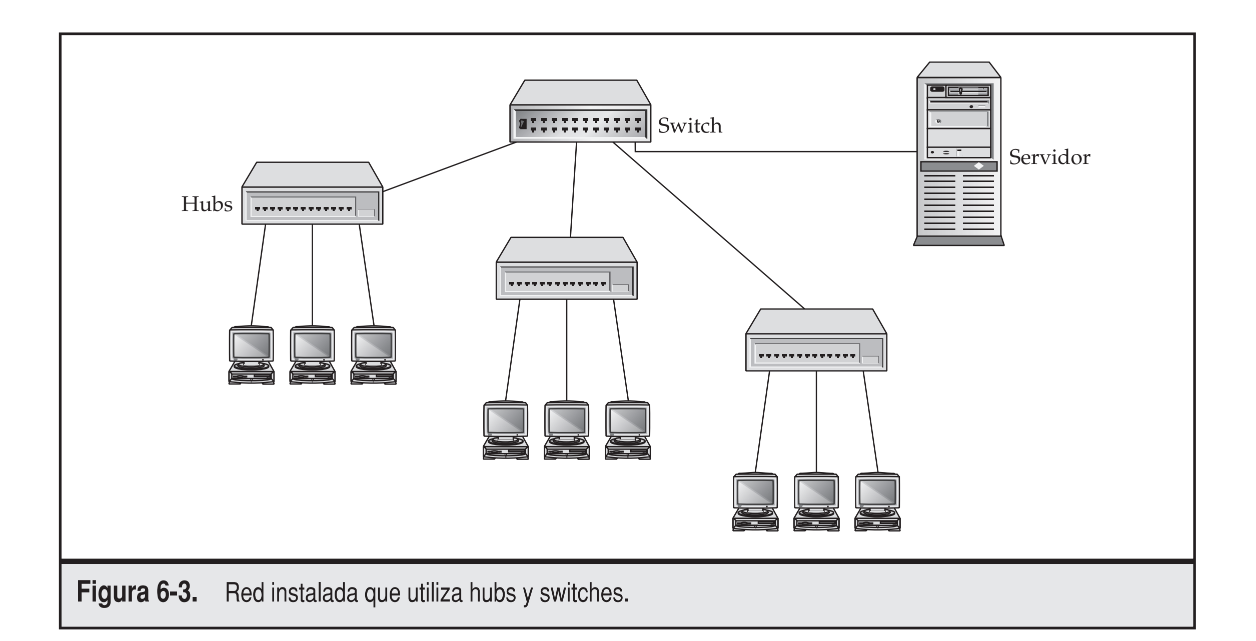


Figura 6-3. Red instalada que utiliza hubs y switches.

tado debido a que los switches, en la actualidad, dominan el mercado ya que tienen los mismos beneficios a un costo mucho más bajo y son mucho menos complejos. Además, la mayoría de las redes actuales evitan los hubs a favor de un diseño basado cien por ciento en switches. De hecho, es virtualmente imposible comprar hubs; todos los fabricantes típicamente ofrecen sólo switches. (A veces, aún se puede comprar hubs muy pequeños, que tengan un número de puertos en el

¿Es mejor utilizar un menor número de hubs grandes o un número mayor de hubs pequeños?

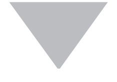
Los hubs más grandes (o switches, como se estila en estos días) en los que pueden residir cientos de conexiones dentro de un solo chasis son, en general, más potentes que sus contrapartes más pequeñas de 24 puertos, y tienden a poseer más redundancia integrada, como fuentes de alimentación de respaldo en la unidad, etc. Sin embargo, algunas veces es más fácil y más barato construir una red utilizando hubs de 24 puertos menores o switches ya que usted simplemente compra una unidad extra de 24 puertos como un respaldo reemplazable (una unidad de respaldo que puede fácilmente reemplazarse para ocupar la posición de la unidad que esté fallando) que usted pueda manualmente implantar en el momento que ocurra una falla. La única desventaja real de este método es que la redundancia no es automática: si un hub/switch de 24 puertos falla, tendrá que mover sus conexiones al hub/switch de respaldo, mientras que una unidad más grande y con mayor redundancia puede conmutarse a características redundantes de manera automática. Como siempre, evalúe con mucho cuidado esos balances para adecuarlos a las necesidades de su compañía en particular.

rango de 4 a 8 pero, incluso en éstas aplicaciones pequeñas, son preferibles los switches y no son muy caros.) Es importante que usted comprenda la diferencia entre los hubs y los switches ya que puede encontrar aún hubs instalados en algunas redes; sin embargo, en las redes más nuevas, encontrará exclusivamente switches. Hacer eso reduce de manera dramática la probabilidad de que se presenten colisiones entre paquetes en la red, lo cual puede suceder en un arreglo basado en hubs.

Puentes

Los *puentes* son, en pocas palabras, versiones de repetidores más inteligentes. Los puentes pueden conectar dos segmentos de red entre sí, pero tienen la inteligencia suficiente para enviar tráfico de un segmento a otro *sólo cuando el tráfico está destinado para ese otro segmento*. Por tanto, los puentes se utilizan para segmentar redes en tramos más pequeños. Se encuentran también disponibles algunos puentes que pueden conectar sistemas de conectividad de redes y medios de transmisión diferentes, como cable coaxial Thin Ethernet y par trenzado Token Ring.

Como puede recordar, los repetidores operan a nivel capa física (capa uno) del modelo OSI para la conectividad de redes. Los puentes trabajan una capa más arriba, en la capa de enlace de datos (capa dos). Los puentes analizan la dirección de control de acceso al medio (MAC) de cada paquete que encuentran a fin de determinar si deben enviar dicho paquete a otra red. Los puentes contienen información acerca de la dirección de todas las partes de su red, a través ya sea de una tabla de enrutamiento estática que usted programa o de un sistema dinámico de aprendizaje tipo árbol que busca automáticamente todos los dispositivos y direcciones en la red.



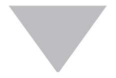
PISTA Debido a que trabajan por debajo de la capa de red en la que se encuentran definidos protocolos como TCP/IP e IPX/SPX, a los puentes no les interesan los protocolos de red que transportan. Lo único que les interesa es la información que se requiere para operar en la capa de enlace de datos, lo que significa que los datos pasan a través del puente y no dependen de su dirección MAC.

Los puentes se deben utilizar solo en redes pequeñas, o en casos donde usted tenga que utilizar un repetidor, pero que se beneficiaría al evitar que tráfico en un segmento se transmitiera en el otro segmento innecesariamente. A menudo los ruteadores o switches ofrecen soluciones que funcionan mejor y crean menos problemas, por lo que examine estas opciones antes de seleccionar un puente.

Ruteadores

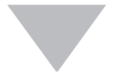
De la misma forma en que los puentes son, básicamente, más inteligentes que los repetidores, los ruteadores son más inteligentes que los puentes. Los *ruteadores* funcionan en la capa de red (capa tres) del modelo OSI y son más inteligentes que los puentes para enviar los paquetes entrantes a su destino final. Debido a que los ruteadores trabajan en la capa de red, cualquier conexión a través del ruteador requiere solo que las capas superiores utilicen los mismos protocolos. Los ruteadores pueden traducir cualquiera de los protocolos de las capas uno a tres a cualquier otro protocolo de las capas uno a tres (siempre y cuando el ruteador haya sido configurado y diseñado para hacerlo). Los ruteadores pueden conectar tanto redes similares como diferentes. A menudo se utilizan en los enlaces de las redes de área amplia (WAN).

En realidad, los ruteadores se convierten en un nodo de la red y tienen su propia dirección de red. Otros nodos envían paquetes al ruteador, que analiza el contenido de los paquetes y los transfiere a donde corresponda. (Por esta razón, con frecuencia los ruteadores están construidos con microprocesadores muy veloces —generalmente basados en computadoras basadas en un conjunto de instrucciones reducidas [RISC]— y una gran cantidad de memoria en ellos a fin de llevar a cabo esta tarea). Los ruteadores también pueden determinar la ruta más corta para alcanzar un destino y la usan. Pueden realizar otros trucos a fin de maximizar el ancho de banda de la red y, de forma dinámica, se ajustan a los problemas cambiantes o patrones de tráfico de una red.



PISTA Para aprender más acerca de las redes a las que están conectados y de lo que deben hacer para enrutar los diferentes tipos de paquetes de manera correcta, los ruteadores utilizan un proceso llamado descubrimiento. Durante este proceso, el ruteador "escucha" cuidadosamente el tráfico en sus puertos y también envía paquetes de advertencia a fin de hacerles saber a los demás dispositivos sobre la presencia de un ruteador.

Los ruteadores forman la espina dorsal de Internet. Cuando usted utiliza el comando TRACERT para rastrear la ruta desde un nodo hacia un destino, la mayoría de las direcciones que aparecen en los saltos son, en realidad, rutas diferentes, cada una de las cuales envía el paquete al nodo siguiente hasta que llega a su destino.



PISTA Los ruteadores solo pueden enrutar protocolos que sean ruteables. AppleTalk, NetBIOS y NetBEUI son ejemplos de protocolos que no son ruteables, mientras que TCP/IP e IPX/SPX sí lo son.

Los ruteadores deben programarse para funcionar de manera correcta. Necesitan tener las direcciones asignadas a cada uno de sus puertos y deben configurarse diferentes parámetros del protocolo de red. Por otra parte, están generalmente programados en una de dos formas. Primero, la mayoría de ellos tiene un puerto RS-232C. Usted puede conectar una terminal o una PC con software de emulación de terminal a este puerto y programar el ruteador en modo texto. Segundo, la mayoría de los ruteadores tiene software basado en red que le permite programar el ruteador, a menudo utilizando herramientas gráficas o una interfase web simple. El método que usted utilice depende del ruteador y sus necesidades de seguridad. (Quizás desee deshabilitar la programación de ruteador basado en la red, a fin de que los usuarios no autorizados no puedan modificar la programación del ruteador). La figura 6-4 muestra un ejemplo de una red que utiliza ruteadores.

Compuertas

Las *compuertas* son interfases de aplicación específica que enlazan las siete capas del modelo OSI cuando son diferentes en uno o todos los niveles. Por ejemplo, si usted necesita conectar una red que utilice uno de los modelos OSI para conectividad de redes a otro que utilice el modelo de IBM Systems Network Architecture (SNA), una compuerta podría realizar esta tarea. Las compuertas también pueden traducir, por ejemplo, de Ethernet a Token Ring, aunque existen soluciones más sencillas que utilizar compuertas si usted necesita dicha conversión. Debido a que las compuertas tienen que realizar muchas traducciones, tienden a ser más lentas que otras soluciones, particularmente, cuando trabajan bajo cargas de tráfico considerables.

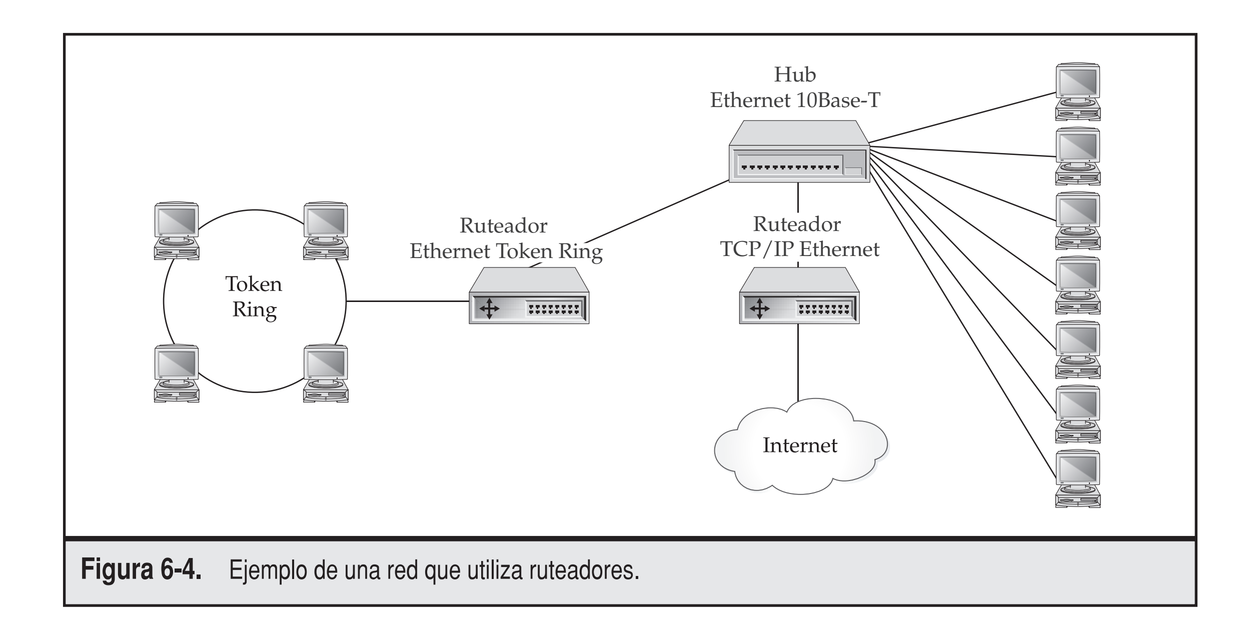


Figura 6-4. Ejemplo de una red que utiliza ruteadores.

En estos días, el uso principal de las compuertas es en el manejo del correo electrónico. POP3 y SMTP son dos ejemplos de protocolos para el manejo de correo que son administrados por compuertas. La mayoría de los sistemas de correo electrónico que pueden conectarse en sistemas disímiles, utilizan una computadora configurada como compuerta para llevar a cabo esa tarea o permiten que el servidor de correo electrónico, por sí mismo, maneje las tareas de las compuertas.

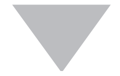
PROTECCIÓN DE UNA RED CONTRA FIREWALLS

Firewalls, estudiadas también en el capítulo 11, son dispositivos de hardware que refuerzan sus políticas de seguridad de la red. En este capítulo también se estudian, porque a menudo se instalan al mismo tiempo que los ruteadores. Por ejemplo, firewalls se instalan a veces con los ruteadores para crear conexiones de interconectividad. En la mayoría de los ruteadores de las oficinas pequeñas u hogareñas, firewall es parte del ruteador en sí mismo. Sin embargo, el equipo de las redes más grandes aún lleva a cabo estas tareas en equipos diferentes.

Firewall es un dispositivo de hardware (que puede ser una computadora configurada para esta tarea en particular, que corra software de firewall o un dispositivo dedicado de firewall que contenga una computadora dedicada) que se instala entre las dos redes y refuerza las políticas de seguridad. En general, firewalls se colocan entre la LAN de una compañía e Internet, pero también pueden utilizarse entre LAN y WAN cuando así convenga.

Existen básicamente dos diferentes tipos de firewalls: basadas en red y basadas en la aplicación. Un firewall basada en red trabaja a nivel paquete y, usualmente, implementa una técnica llamada *filtrado de paquetes*, que permite que éstos entre las redes se comparen con un conjunto de reglas programadas en firewall antes de que se les permita a los paquetes cruzar la frontera entre las dos redes.

Las reglas del filtrado de paquetes pueden admitir o rechazar paquetes que estén basados en la dirección fuente o la dirección destino, o basados en un puerto TCP/IP. Por otro lado, por lo general la aplicación basada en firewalls actúa en un papel proxy entre las dos redes, de forma que no circule tráfico *directamente* entre las dos redes. En lugar de ello, firewall (generalmente llamada *firewall proxy*) actúa como un proxy para que los usuarios de una red interactúen con los servicios de otra red. Esta interacción proxy, en general, se lleva a cabo mediante una técnica llamada *traducción de las direcciones de red (NAT)*, donde las direcciones de la red en la red interna no están expuestas directamente a la red externa. En el modelo basado en la aplicación, firewall proxy se encarga de traducir las direcciones a fin de que se puedan llevar a cabo las conexiones.



NOTA Firewalls no son una panacea para la seguridad de la red. La mejor firewall del mundo no protegerá su red de las amenazas de seguridad, como las que se estudian en el capítulo 11. Sin embargo, son una parte importante de la seguridad, en particular, de las LAN conectadas a Internet.

Firewalls vienen en todas las formas y tamaños y varían en costo desde algunos cientos hasta miles de dólares. En realidad, estos días uno puede comprar pequeñas firewalls personales para el hogar que cuesten menos de 200 dólares para dispositivos basados en hardware o de 40 dólares para software de firewall que puede instalarse en una computadora personal. Los diferentes dispositivos de firewall tienen distintas características y abarcan tanto técnicas basadas en red como basadas en la aplicación para proteger la red. Firewalls también sirven como punto de auditoría del tráfico entre las dos redes, utilizando herramientas de acceso y reporte a fin de que éstas ayuden al administrador a detectar y tratar el tráfico de red inapropiado.

CONEXIÓN DE DISPOSITIVOS RS-232 CON MÓDEMS DE CORTO ALCANCE

A pesar de que algunas personas consideran que el módem de corto alcance no es, en verdad, un dispositivo de red, es un dispositivo necesario para su red a fin de que pueda ofrecer conectividad punto a punto entre una estación de trabajo o terminal y otro dispositivo. Los módems de corto alcance (a menudo llamados *controladores de línea*), le permiten a usted conectar entre sí dos dispositivos RS-232C distantes. Los cables estándar RS-232C tienen un límite en cuanto a distancia de 50 a 100 pies. Los módems de corto alcance permiten que la misma conexión recorra una distancia de 5 millas utilizando un cable telefónico de par trenzado simple.

A menudo, los módems de corto alcance son soluciones perfectas cuando una computadora necesite acceso por terminal a un dispositivo remoto. Por ejemplo, un usuario puede necesitar acceder a una terminal en un sistema telefónico PBX, que utilice un puerto RS-232C. Usted tiene dos opciones para ofrecer este acceso remoto: puede instalar módems convencionales en cada extremo y utilizar una conexión telefónica para conectar la estación de trabajo al PBX, o emplear dos módems de corto alcance e instalar un cable de par trenzado entre los dos puntos. De acuerdo con qué frecuencia se necesite el acceso y qué tan lejos se encuentre el dispositivo, cualquier forma es válida. En general, los módems de corto alcance son más convenientes cuando los dos dispositivos a veces o siempre necesiten estar conectados e instalar un cable de par trenzado entre los dos puntos no sea demasiado costoso o difícil. Los módems de corto alcance son muy baratos, pues cuestan aproximadamente 100 dólares cada uno.

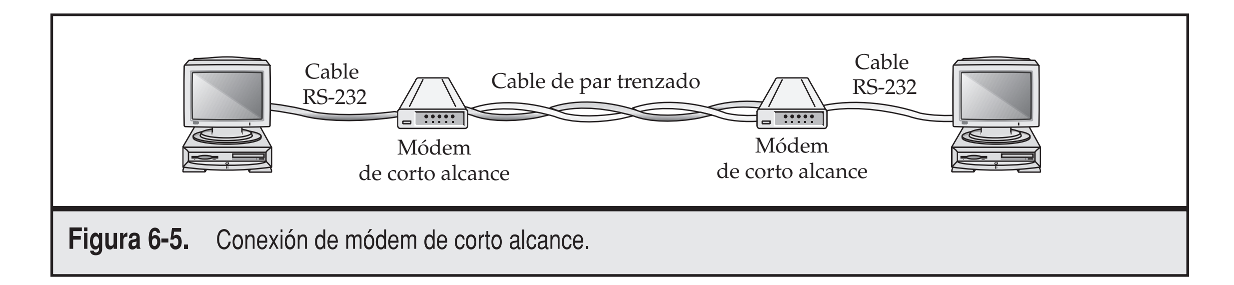


Figura 6-5. Conexión de módem de corto alcance.

En la mayoría de los módems de corto alcance, dos pares de alambre conectan cada módem de corto alcance, aunque existen variantes de un solo par. En la variante de dos pares, un par se utiliza para transmitir datos y el otro para recibirlos. La mayoría de los módems de corto alcance son full duplex, lo cual permite que la transmisión se lleve a cabo en ambas direcciones de manera simultánea.

Para enlazar dos dispositivos mediante módems de corto alcance, debe utilizar un cable estándar RS-232C para conectar cada dispositivo a su módem de corto alcance. Después, usted instala el alambre de par trenzado a un módem de corto alcance utilizando las instrucciones que vienen con el módem. Por último, la mayoría de los módems de corto alcance necesitan alimentación externa, por lo que necesita un contacto de energía para conectarlos. La figura 6-5 muestra un ejemplo de una conexión por módem de corto alcance.



PISTA Si a menudo usted hace interfases con la RS-232C, debe invertir en un dispositivo llamado caja de conexiones. Éste tiene dos conectores RS-232C en cada extremo. En la caja, cada una de las señales RS-232C se representa por medio de un diodo emisor de luz (LED). Tiene postes de parcheo especiales y switches que le permiten reconfigurar la conexión RS-232C en caliente. Las cajas de conexiones son de gran utilidad para lograr comunicación RS-232C entre dos dispositivos que no se están comunicando, muestran qué está pasando en realidad con las señales y le permiten a usted probar diferentes configuraciones del cable de manera dinámica. Una vez que utilice la caja de conexiones para darse una idea de cómo se comunican los dispositivos, entonces, se puede fabricar un cable permanente con esas especificaciones.

RESUMEN DEL CAPÍTULO

En este capítulo usted aprendió acerca de los elementos de hardware clave que conforman la mayoría de las redes. Es importante que esté familiarizado con las capacidades de estos tipos de hardware de red, que deben formar la base de cualquier diseño de red o esfuerzo para ponerla a tono. Mientras que es muy extenso el estudio del hardware que aprendió aquí, no es el último de los tipos de hardware de red acerca del cual es necesario que usted sepa. En otros capítulos de este libro se estudia hardware de red adicional muy importante. En particular, usted también debe saber acerca del hardware para el acceso remoto, del que soporta enlaces WAN y acerca de ciertas funciones de red que se llevan a cabo en diferentes tipos de servidores de red.

En el capítulo 7 se estudian las diferentes tecnologías utilizadas para conectar redes entre sí, en general, separadas por grandes distancias. Las conexiones WAN se utilizan para conectarse a Internet y también para establecer conexiones de tiempo parcial y completo entre LAN, como en el caso de las instalaciones de una compañía a otras instalaciones de la misma.

CAPÍTULO 7

Conecciones entre WAN

Muchas compañías que tienen presencia en diferentes áreas geográficas necesitan compartir recursos. Por ejemplo, quizás el sistema de contabilidad de la compañía opera en el edifico de la casa matriz donde se ubica el departamento de contabilidad y el grupo que maneja los sistemas administrativos de información (MIS), pero la bodega que se encuentra del otro lado de la ciudad necesita acceder al sistema de contabilidad para llenar tarjetas del inventario, ingresar datos y tareas relacionadas con el surtido de órdenes.

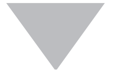
Quizá la compañía utiliza un sistema de trabajo en grupo como Lotus Notes, el cual necesita actualizarse regularmente en cuanto a información y mensajes de un sitio a otro. En el mundo real, la situación puede hacerse aún más compleja. Algunas empresas tienen oficinas alrededor del mundo, y cada una debe cubrir requerimientos diferentes para acceder y actualizar datos en otros puntos.

Todas éstas son situaciones en las que puede ser útil una *red de área amplia (WAN)*. Es verdad que en una situación de apuro, las diferentes oficinas podrían enviar y recibir datos entre sí mediante Federal Express y máquinas idénticas de cinta, discos CD-R, discos zip, JAZ u otro medio y simplemente enviar los datos de un lado a otro (se supone que la aplicación soporta el intercambio de datos de esta forma). Sin embargo, este tipo de escenario tiene algunas desventajas, la principal es que, comparativamente, es muy lento.

Existen muchas formas de conectar LAN que estén en un lugar con LAN que se encuentren en otro sitio. Llevar a cabo dichas conexiones es el tema de este capítulo. Primero, usted aprenderá acerca de los conceptos involucrados en enlazar LAN para formar una WAN. Después, estudiará diferentes tecnologías de WAN junto con los compromisos relativos que cada una requiere.

DETERMINACIÓN DE LAS NECESIDADES DE LA WAN

Excepto contados casos, los enlaces WAN son casi siempre muy costosos de conservar, en particular debido a que las necesidades de ancho de banda aumentan con el tiempo. Por ello, existe la tendencia por expandir el ancho de banda, pero estas mejoras son muy costosas. Además, los enlaces WAN son, en general, mucho más susceptibles de presentar problemas en comparación con las LAN debido a que existen muchos puntos de falla adicionales. Por estas razones, antes de que seleccione, es importante que analice, con mucho cuidado, la necesidad de una WAN y después estudie las opciones disponibles, sus costos y los compromisos que están involucrados. Los costos pueden variar ampliamente entre las diferentes tecnologías, las velocidades y otros factores (entre ellos, la ubicación de sus oficinas), así que tiene que depender de manera notable de la información sobre costos y disponibilidad proporcionados por sus proveedores locales para realizar su propio análisis de la WAN. Además, los costos y la disponibilidad cambian casi cada semana, así que asegúrese de obtener datos actualizados de sus proveedores locales antes de comprometerse con una tecnología de WAN en particular.



PISTA A menudo, la necesidad de una WAN puede satisfacerse mediante una tecnología llamada redes privadas virtuales (VPN). Una VPN es una red privada que se crea mediante una red pública, típicamente Internet. Una VPN se llama “privada” debido a que todos los paquetes entre dos puntos están encriptados, por lo que a pesar de que los paquetes se transmiten a través de una red pública, su información se conserva segura. Además, debido a que las VPN utilizan Internet, en general son más baratas que los enlaces WAN dedicados y, a menudo, pueden usar las conexiones existentes de Internet en dos (o más) puntos. Las VPN se estudian con detalle en el capítulo 10.

Análisis de los requerimientos

Antes de revisar las diferentes tecnologías WAN, debe tener una firme idea de la necesidad de contar con una de ellas. Debido al costo y al tiempo requerido para implementar y mantener una WAN, usted no querrá instalar una, hasta que en realidad exista una necesidad para ello.

La primera WAN de una compañía, generalmente, la impone una aplicación en particular, como un sistema de contabilidad. Después, una vez que la WAN se encuentra en operación, la compañía comienza a utilizarla para otras aplicaciones. Por ejemplo, una compañía puede estar transfiriendo correo electrónico de un punto a otro mediante líneas conmutadas, pero una vez que se ha instalado la WAN que soporta el sistema de contabilidad, es más fácil enrutar el correo electrónico mediante un enlace WAN que conservar dos esquemas de conexión independientes. Otros usos de la WAN se presentan de esta forma, por lo que es importante analizar a fondo la aplicación principal y, después, considerar qué otros usos se le puede dar. Si usted no toma en cuenta todos los usos que la compañía pueda darle, podrá notar que ha invertido una gran cantidad de dinero en una solución que, en realidad, no satisface todas sus necesidades.

Usted necesita responder una serie de preguntas antes de considerar las diferentes opciones de las WAN:

- ¿Cuáles son las sucursales, filiales, oficinas, etc. que participarán en la WAN y qué tipo de servicios se encuentran disponibles en dichos puntos? Por ejemplo, es muy poco probable que una oficina de ventas en Tahiti compre una línea xDSL.
- ¿Cuántos datos es necesario transferir de un sitio a todos los demás y en cuánto tiempo?
- ¿Qué tan rápido necesitan transferirse los datos?
- La transferencia de datos, debe ser síncrona o asíncrona? Por ejemplo, el dependiente de la bodega que ingresa los registros directamente al sistema de contabilidad ubicado en otro sitio requiere de una conexión síncrona (en tiempo real), mientras que un restaurante que necesite cargar la información sobre las ventas en la oficina matriz a una determinada hora por la noche, solo requiere de una conexión asíncrona.
- ¿Cuándo es necesario llevar a cabo las transferencias de datos? ¿Ocurren todo el tiempo? ¿Necesitan ocurrir una vez cada 30 minutos, o seguir alguna otra programación?
- ¿Cuáles son las restricciones de presupuesto y cuáles son los costos de las diferentes alternativas disponibles?

Una vez que tenga las respuestas podrá responder las preguntas que lo guiarán hacia una tecnología WAN en particular. Estos temas se estudian en las secciones siguientes.

¿Conmutado o dedicado?

Un *enlace* WAN conmutado es uno que no está activo todo el tiempo. Por ejemplo, una conexión por módem por línea telefónica desde un lugar a otro sería una conexión conmutada. Otro ejemplo es una conexión ISDN de un punto a otro. Éstos son ejemplos de conexiones que se forman solo cuando las necesita y generalmente paga por el tiempo que la conexión estuvo abierta, en

lugar de pagar por la cantidad de datos que pueda transmitir a través de la conexión. La figura 7-1 es un ejemplo de un enlace WAN conmutado.

Los enlaces conmutados pueden estar basados en la conexión o en el paquete. Un *enlace conmutado basado en la conexión* forma un enlace a medida que se necesite y aparta una cantidad disponible de ancho de banda en el mismo. Un *enlace conmutado basado en paquetes* envía bloques de datos hacia una nube de red en la que puede seguir un gran número de trayectorias a su destino, para después salir de la nube. Este último tipo de redes puede ser más confiable debido a que los datos pueden tomar muchas trayectorias diferentes, pero nadie le puede garantizar que todos los paquetes vayan a llegar en algún momento determinado. Un enlace conmutado basado en la conexión solamente le proporciona una "tubería" de la fuente al destino, pero usted puede controlar lo que viaja por la tubería y cuánto tiempo le toma llegar a su destino.

Un enlace WAN *dedicado* siempre se encuentra disponible y listo para transmitir. Algunos ejemplos de conexiones WAN dedicadas son las líneas DS1 (T-1), las líneas *x*DSL y las líneas telefónicas privadas. Usted utiliza una conexión dedicada cuando necesita que esté disponible todo el tiempo o cuando se justifica desde el punto de vista económico que esa conexión sea más barata que un enlace conmutado. La figura 7-2 muestra un enlace WAN dedicado.

¿Privado o público?

Una *red privada* es una red que es propiedad de determinada compañía. Ningún dato de cualquier otra compañía puede enviarse a través de esa red privada. Las ventajas son que los datos están seguros, que puede tener control acerca de cómo se utiliza la red y puede predecir cuánto ancho de banda tiene disponible. Una *red pública* (o *red externa*), como Internet, es a través de la cual circulan datos de muchas compañías. Las redes públicas son menos seguras que las privadas, pero las ventajas de las redes públicas estriban en que son mucho menos costosas y no tiene que mantener la red externa.

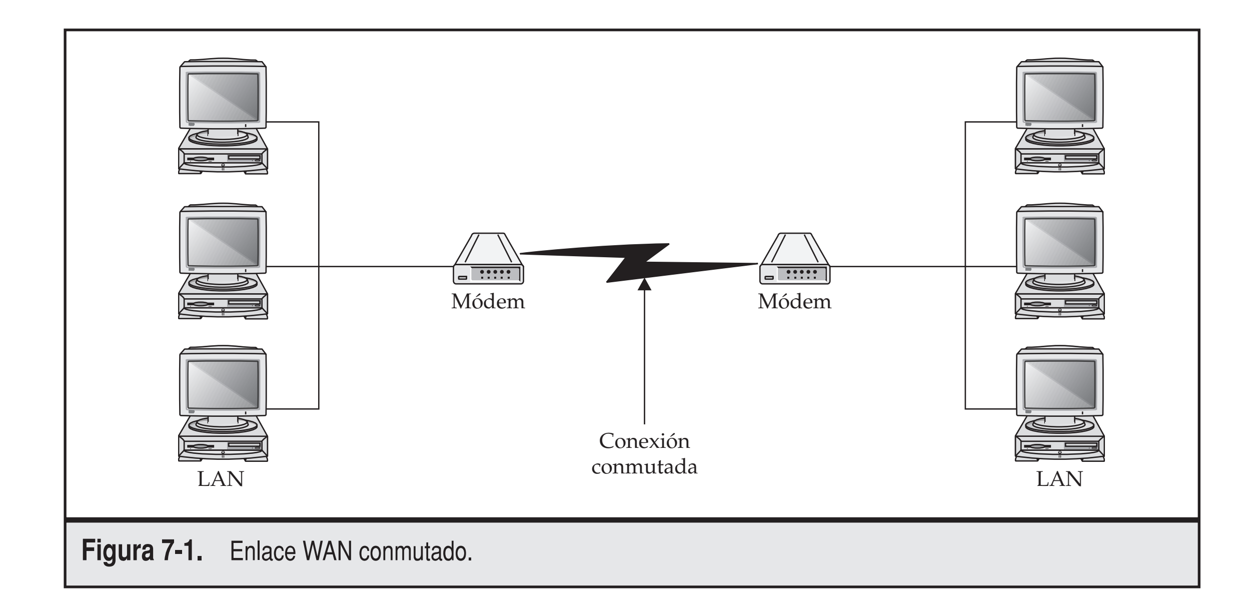


Figura 7-1. Enlace WAN conmutado.

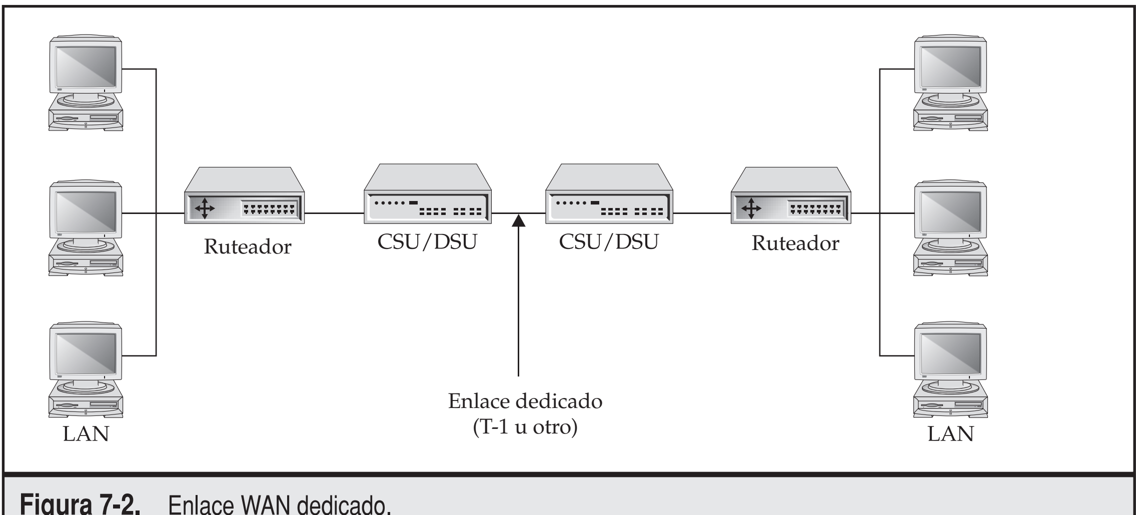


Figura 7-2. Enlace WAN dedicado.

Utilice una red pública si:

- No le importa si, de vez en cuando, le toma más tiempo a los datos alcanzar su destino o si la demora entre los sitios es relativamente impredecible.
- Busca el menor costo de conexión a la red posible.
- Los datos no requieren seguridad o usted tiene capacidad para otorgarles seguridad en su viaje a través de la red pública. (Existen tecnologías que pueden proporcionar dicha seguridad, como las redes privadas virtuales o algún tipo de encriptado de datos).

Utilice una red privada bajo estas condiciones:

- La seguridad de los datos es de primordial importancia.
- Usted cuenta con un gran número de asesores con experiencia para configurar y mantener la red pública.
- El costo no tiene mucha importancia en relación con los beneficios que trae la red.
- Usted necesita control total y confiable en cuanto al uso del ancho de banda de la red.

TIPOS DE CONEXIÓN DE LA WAN

Ahora que comprende algunas de las bases de los enlaces WAN, en lo que resta de este capítulo le proporcionaremos un panorama de las diferentes tecnologías disponibles de WAN y le ofreceremos pistas y consejos sobre cada tipo de enlace.

Servicio telefónico convencional (POTS)

El servicio telefónico convencional (POTS) es el que todo el mundo conoce. Aunque no está calificado técnicamente como una conexión WAN (al menos como la mayoría de la gente piensa de las WAN), POTS puede incluso servir para enlazar dos o más sitios entre sí para cubrir ciertas necesidades de poco ancho de banda. Aunque se encuentra entre los métodos más lentos para establecer una conexión de red, POTS está presente en todas partes y se utiliza fácilmente en todo el mundo. Además, es también, en general (¡pero no siempre!), la forma más barata de conectarse.

El servicio POTS se transporta a través de un conjunto de alambres de par trenzado (en otras palabras, solo dos alambres). En algunos casos, se utilizan dos conjuntos de alambres de par trenzado, pero se utilizan solo los dos alambres principales para transferir la señal de teléfono y las señales de timbrado. Los otros dos se utilizan para otras cosas, como para proporcionar iluminación al tablero del teléfono o para ofrecer una luz de mensaje en espera en algunos sistemas de PBX. Las conexiones POTS actualmente utilizan simples conectores telefónicos RJ-11, que se conectan a presión de una manera muy sencilla.

La velocidad teórica máxima del servicio POTS analógico básico es de 33.6 Kbps. Muchos factores pueden hacer que esta velocidad disminuya; el más importante es la calidad de la línea. Las líneas telefónicas con estática, típicamente no se conectan a la velocidad límite de 33.6 Kbps, pueden perder la conexión repentinamente, los datos que se tratan de transmitir o detenerse por periodos excesivos ya que las ráfagas de estática anulan su capacidad para transferir datos.

Cuando utiliza POTS para establecer una conexión de red, es muy recomendable tener módems acoplados en ambos extremos de la línea. Los módems acoplados del mismo fabricante pueden negociar más fácilmente la velocidad de transmisión de datos más alta posible y, a menudo, pueden soportar modos "hacia abajo", los cuales utilizan de manera automática una velocidad más baja cuando el ruido en la línea se convierte inesperadamente en un problema.

El servicio POTS transmite señales analógicas, no digitales. Los datos enviados entre sistemas se convierten de datos digitales a datos analógicos mediante el empleo de un módem. La palabra *módem* es, en realidad, la sigla que se basa en la función del dispositivo: modulador/demodulador. En cada extremo de la conexión, el módem del sistema modula la señal digital en una señal analógica y la envía a través de la línea telefónica, como una serie de sonidos audibles. Después, en el extremo receptor, el módem demodula la señal analógica audible convirtiéndola en datos digitales para que los pueda utilizar la computadora.

Red digital de servicios integrados (ISDN)

La tecnología de la Red Digital de Servicios Integrados (ISDN), una red de comunicaciones digitales de alta velocidad que se basa en los servicios telefónicos actuales, ha estado en el mercado por más de diez años. Sin embargo, debido a las mejoras extensivas que se requieren en las centrales telefónicas (CO) de la compañía, el servicio ISDN no ha estado disponible ampliamente sino hasta años recientes, y aun ahora, generalmente solo se encuentra en grandes áreas metropolitanas.

ISDN se presenta en dos formas básicas: la Interfase a velocidad básica (BRI) y la Interfase a velocidad principal (PRI). La conexión ISDN-BRI está conformada por tres canales. A dos canales se les llama *canales del suscriptor* y transportan datos a velocidades de 64 Kbps por canal. Los canales del suscriptor también pueden transportar llamadas de voz, esto es, llamadas telefónicas

comunes. (Cada canal del suscriptor puede transportar una llamada de voz a la vez). El tercer canal, llamado *canal de datos*, transporta información acerca del establecimiento de la llamada y otras comunicaciones de control necesarias para administrar los dos canales de suscriptor. El canal de datos transporta 16 Kbps de datos. Los canales del suscriptor se abrevian como *canales B*, mientras que los canales de datos se abrevian como *canal D*. Por tanto, a una conexión ISDN-BRI a menudo se le conoce como conexión 2B+D, lo cual refleja el número y tipo de canales que contiene.

Una ISDN-PRI está formada por 24 canales B y un canal D. Una conexión PRI puede transportar un total de 1.544 Mbps, exactamente igual que una línea T-1.

NOTA Diferentes tipos de configuraciones PRI se encuentran disponibles en varias partes del mundo. La configuración llamada 24B+D es común, y es posible que usted también vea variaciones como 22 canales B con un canal D a 64 Kbps, 24 canales B a 56 Kbps o aun 30 canales B estándar (lo que hace un total de 1.92 Mbps).

Las conexiones ISDN se forman, generalmente, a medida que se necesitan: están conmutadas. Para emplear ISDN para un enlace WAN, usted utiliza ruteadores ISDN por demanda en cada extremo, los cuales pueden "marcar" el otro ruteador cuando los datos estén pendientes. Debido a que ISDN tiene unos tiempos de establecimiento de la llamada extremadamente altos, las conexiones ISDN se forman más rápido que las conexiones POTS: toma menos de un segundo.

NOTA ISDN es el tipo de conexión más común en sistemas de videoconferencia; aunque muchos sistemas también pueden utilizar Internet, la mayoría de las compañías confían en ISDN como su principal tipo de conexión para llamadas de videoconferencia. Si usted desea instalar un sistema así, debe pensar en la instalación de al menos dos conexiones BRI (tres es mejor) y en la compra de un sistema de videoconferencia que soporte al menos 256 Kbps de ancho de banda. Las llamadas por videoconferencia a través de un solo BRI (128 Kbps) son muy pobres en cuanto a calidad; dos BRI (256 Mbps) es mucho mejor y las conexiones de tres BRI (384 Kbps) son excelentes. Observe también que es necesario que en ambos extremos de la llamada haya soporte de la misma velocidad y número de BRI.

ISDN no ha sido tan ampliamente adoptado como se esperó; ha sido opacado por *x*DSL y otros tipos de conexión que ofrecen mejores características de precio/desempeño. Los cambios de precio ocurren de manera regular. Los precios de ISDN también varían considerablemente en diferentes partes del país. Es importante que usted obtenga información completa acerca de las tarifas de su propia compañía regional Bell (RBOC) antes de que seleccione ISDN. Después, utilizando sus datos de proyección del uso, calcule el costo de utilizar ISDN.

En general, la instalación de una línea ISDN-BRI, bajo el supuesto de que no son necesarias modificaciones en el cableado, cuesta aproximadamente 150 dólares. Algunas RBOC podrían exentarlo del cargo por la instalación si firma un acuerdo en el que se comprometa a conservar la línea ISDN por un periodo de uno a dos años.

PISTA En algunas partes de Estados Unidos, en ocasiones la instalación de una línea ISDN toma una cantidad considerable de tiempo: hasta dos meses en algunos casos. Antes de seleccionar ISDN, obtenga de su RBOC una estimación lo más precisa posible y por escrito, acerca de cuándo podrá terminar la instalación. Asegúrese de estar prevenido para el caso de que la RBOC no cumpla con la fecha de terminación.

Los cargos mensuales por ISDN son similares a los de POTS. Los cargos por las llamadas de larga distancia también. Sin embargo, recuerde que conectarse a través de dos canales B es equivalente a hacer dos llamadas por separado y que cualquier cargo que exista de una sola llamada se duplicará cuando utilice ambos canales B.

Línea digital de suscriptor (DSL)

Un tipo relativamente nuevo de conexión que comienza a estar disponible se conoce con el nombre de línea digital de suscriptor (DSL). Existe un gran número de “sabores” diferentes de DSL; cada nombre comienza con una inicial diferente o combinación de éstas, lo cual explica por qué a menudo a DSL se le llama *x*DSL. Dentro de las variantes se incluyen las siguientes:

- **ADSL** El servicio DSL asimétrico permite que se puedan recibir hasta 8 Mbps de datos y se puedan enviar hasta 1 Mbps de datos. Muchos RBOC ofrecen solo hasta 1.5 Mbps en la recepción (lo cual se llama en dirección *hacia abajo*) y 256 Kbps en el envío (lo cual se llama en dirección *hacia arriba*), pero la distancia desde la central telefónica puede afectar las velocidades disponibles en cualquier punto en particular. Para distancias mayores, debe haber conexiones disponibles solamente a velocidades mucho más bajas (aunque en todos los casos las conexiones ADSL son aún más rápidas que las POTS que utilizan un módem).
- **HDSL** El servicio DSL de alta velocidad (HDSL) permite la conexión de dos sitios a una velocidad de entre 768 Kbps y 2.048 Mbps.
- **RADSL** El servicio DSL de velocidad adaptable (RADSL) permite una velocidad de datos de 600 Kbps a 12 Mbps en la recepción y de 128 Kbps a 1 Mbps en la transmisión.
- **SDSL** El servicio DSL simétrico (SDSL) permite velocidades bidireccionales que varían desde 160 Kbps a 2.048 Mbps.
- **VDSL** El servicio DSL a muy alta velocidad (VDSL) permite hasta 26 Mbps de ancho de banda.
- **ISDL** La velocidad del DSL basado en ISDN (IDSL) es aproximadamente la misma que la de ISDN, pero IDSL se utiliza casi exclusivamente para datos, ya que es una conexión hacia un solo destino y siempre está disponible, en contraposición con ISDN, la cual puede utilizarse para realizar llamadas a otras conexiones ISDN.

En esta sección, usted aprendió cómo trabaja *x*DSL y cuándo puede implantar sus capacidades de extremado ancho de banda. En estos análisis me he enfocado en ADSL debido a que es la que prevalece y la menos costosa. Sin embargo, para los enlaces WAN, debería enfocarse en SDSL si sus necesidades de datos de WAN son similares en ambas direcciones.

Cómo trabaja xDSL

El alambre de cobre de par trenzado que transporta el servicio POTS puede transportar señales de hasta 1 MHz de frecuencia. Sin embargo, POTS utiliza solamente 8 kHz de ese ancho de banda de frecuencias. La razón de esta limitación es que, en el switch de la central telefónica (CO), hay una

tarjeta que interfasa con la señal analógica que el par trenzado envía a la red digital de la compañía telefónica. Esta tarjeta de interfase permite solo 4 KHz de frecuencias de señalización en cada dirección, a pesar de que el mismo cable puede transportar un rango de frecuencias mucho más amplio.

*x*DSL funciona abriendo ese ancho de banda de 1 MHz máximo mediante el uso de tarjetas de interfase *x*DSL que la RBOC puede instalar en el switch de la central telefónica. En el caso de las líneas que se conectan a esas tarjetas, el nuevo rango de frecuencias puede transportar mucho más datos que si la tarjeta no estuviera instalada. Sin embargo, la distancia del equipo de la computadora al switch de la central telefónica limita la velocidad de transferencia. La mayor parte de las implantaciones *x*DSL funcionan de manera óptima hasta 3658 m (aproximadamente 2 millas). En particular, es posible alcanzar las velocidades de transferencia de 8 Mbps en la recepción y 1 Mbps en el envío de datos de ADSL solo a una distancia de 3658 m de la central telefónica. Son posibles distancias mayores, pero no a la mayor velocidad de transferencia de datos posible. Por ejemplo, operar una conexión ADSL a 5486 m —la distancia a la que se encuentra 95% de los teléfonos con respecto al switch de la central telefónica— degrada el desempeño a 1.5 Mbps, en el mejor de los casos, en la dirección de recepción. Se estima que solo 50% de los hogares de Estados Unidos se encuentran dentro de los 3658 m de un switch en una RBOC. La buena noticia es que existen nuevas implantaciones de *x*DSL que pueden superar el limitante en cuanto a distancia.

ADSL

Como se mencionó, el ADSL puede soportar hasta 8 Mbps de recepción de datos (también llamados *datos de bajada*) y hasta 1 Mbps en el envío de datos (también llamados *datos de subida*). Además de estos dos canales de datos, el servicio ADSL cuenta con un canal de 8 KHz para POTS, que puede coexistir con los canales de datos ADSL.

¿Por qué DSL asimétrico?

Muchas necesidades de acceso a datos son asimétricas. En otras palabras, en cualquier momento, un sistema puede necesitar recibir más datos de los que necesita enviar o viceversa. La mayoría de las conexiones de acceso remoto, en particular las de Internet, son asimétricas. Lo importante es ser capaz de recibir datos de una manera rápida, más que enviarlos más rápido.

Debido a lo anterior, ADSL es la implantación de *x*DSL más popular entre las demás implantaciones, simplemente porque ofrece más beneficios con la misma cantidad de ancho de banda total. La mayoría de las aplicaciones trabajarán mejor cuando la velocidad de los datos sea mayor hacia abajo que hacia arriba.

Algunas implantaciones de *x*DSL son simétricas, como el DSL simétrico y el DSL de alta velocidad. Estos tipos de conexión *x*DSL son más adecuados para usos donde el intercambio de datos es, a groso modo, igual en ambas direcciones, como el caso de dos LAN remotas conectadas entre sí.

Las implementaciones específicas de ADSL varían en su velocidad de transmisión de datos. Algunas de las implantaciones más lentas funcionan solo a 1.5 Mbps hacia abajo y 256 Kbps hacia arriba. En algunos casos, esta velocidad puede aun descender a 384 Kbps hacia abajo y a 64 Mbps hacia arriba.

Existe mucho interés alrededor de *x*DSL, en particular en ADSL. El costo por megabyte de datos transmitidos es mucho menor que el servicio POTS y es incluso considerablemente menos costoso que ISDN. En la actualidad, *x*DSL está disponible en la mayoría de las ciudades de Estados Unidos.

Conexiones T-1/T-3 (DS1/DS3)

Hace más de 40 años, los Laboratorios Bell desarrollaron una jerarquía de sistemas que podían transportar señales de voz digitales. En el nivel más bajo de esta jerarquía se encuentra una conexión llamada *conexión DS0*, la cual transporta 64 Kbps de ancho de banda. A una conexión formada por 24 canales DS0 se le llama DS1, la cual transporta hasta 1.544 Mbps cuando todos los canales se encuentran en uso. Al siguiente nivel se le conoce como *DS3*, y transporta 672 canales DS0, para formar un agregado de 44.736 Mbps. A la conexión DS1 se le llama comúnmente *conexión T-1*, la cual, en realidad, se refiere al sistema de repetidores que pueden transportar el tráfico DS1 a través de una conexión de cuatro pares de par trenzado. (Es sorprendente que un DS1 requiera solo dos pares de par trenzado y no un cable de fibra óptica o algo más exótico. Para comprender qué cantidad de datos puede transportarse a través de un solo alambre telefónico, consulte la sección anterior, "Línea de Abonado Digital [DSL]").

Las conexiones DS1 se utilizan comúnmente como conexiones digitales entre el PBX de una compañía y un punto de presencia (POP) de una telefónica de larga distancia, y se utilizan con mucha frecuencia para conectar LAN a Internet. Una conexión DS1 puede manejar hasta 24 llamadas de voz o unas 24 conexiones de datos de forma simultánea. Por otra parte, utilizando un multiplexor y un DS1, usted puede formar una conexión grande a 1.544 Mbps.

Existe también una tecnología muy popular conocida con el nombre de *T-1 fraccional*, donde se instala un DS1 completo, pero solo el número de canales que usted paga se ponen a operar y éstos se encuentran disponibles para su uso. T-1 fraccional es espléndido, ya que compra solo el ancho de banda que necesita y si desea incrementarlo (hasta un máximo de un DS1) solamente tiene que llamar por teléfono (y tener algunos dólares) disponibles.



NOTA Las conexiones WAN DS0, DS1 y DS3 utilizan la tecnología de señalización de frame relay en el lado RBOC de la conexión. Comprender todos los detalles de frame relay no es importante, aunque usted debe saber que cuando instale una conexión DS*x* a Internet para su LAN, en realidad está utilizando los servicios que proporciona frame relay.

En el extremo de la conexión DS1 están dos piezas de equipo fundamentales: un CSU/DSU que convierte las señales DS1 en señales de la red, y un ruteador que envía paquetes entre el DS1 y la LAN.

Modo de transferencia asíncrona (ATM)

El modo de transferencia asíncrona, comúnmente llamado ATM, es una tecnología que desarrolla muy alta velocidad para la transmisión de datos entre dos puntos. ATM es una tecnología de conectividad multiplexada que agrupa datos para formar entidades llamadas *celdas* y des-

pués transmite éstas a través de una conexión de red ATM. Las redes ATM pueden transportar tanto voz como datos. ATM es muy rápida, con velocidades que fluctúan desde 155 Mbps a 622 Mbps. En general, se utiliza solo en compañías relativamente grandes que necesiten gran velocidad para sus enlaces WAN o por empresas que necesiten enviar cantidades enormes de datos a través de una conexión de red, por ejemplo, que deba transmitir una gran cantidad de datos de video.

X.25

Las conexiones X.25 han estado disponibles por mucho tiempo, pero por lo general no se utilizan en conexiones WAN tanto por el envío de información de control que involucra, como por el compromiso entre el precio y el ancho de banda que no es competitivo respecto a otras soluciones. Sin embargo, algunas redes más antiguas pueden tener conexiones X.25 instaladas y, de hecho, se utilizan mucho en Europa. X.25 es una conexión WAN de conmutación en paquetes, que permite que los datos viajen a través de la nube X.25, que trabaja de manera similar a Internet, pero que utiliza una red X.25 privada/pública. Las conexiones X.25 son relativamente lentas (56 Kbps), pero en algunos casos pueden ser más rápidas.

El ejército de Estados Unidos desarrolló y diseñó X.25 para permitir el tráfico de voz después de un ataque nuclear. Como puede adivinar a partir de lo anterior, X.25 es un protocolo seguro y extremadamente confiable para la transmisión de datos. Todas las tramas (similares a los paquetes) que se envían a través de las redes X.25 se verifican en su totalidad de un extremo de la conexión al otro.

RESUMEN DE CAPÍTULO

En este capítulo, usted aprendió acerca de los conceptos y las tecnologías relacionadas con los enlaces de las redes de área amplia, entre ellos los diferentes tipos de enlaces y conexiones, así como la forma de especificar un tipo de tecnología WAN en particular para una determinada aplicación. Mientras que el número de opciones puede hacer confusa esta área, el proceso se facilita si el problema se divide en partes más pequeñas. Básicamente, asegúrese de realizar un trabajo minucioso y con mucho cuidado al identificar sus necesidades de una WAN, y después consulte varios proveedores de esta tecnología de su área, a fin de analizar de qué forma las soluciones que le propongan satisfacen sus necesidades.

En el capítulo siguiente se estudian los protocolos de red, como TCP/IP e IPX/SPX. Usted aprenderá cómo trabajan, cómo se construyen sus paquetes y las diferentes características de cada tipo de protocolo de red. También aprenderá acerca de otros protocolos comunes, en particular, los asociados con TCP/IP, como el SMTP, el HTTP y el WINS.



CAPÍTULO 8

Protocolos de conectividad de redes

Un *protocolo* de red es un conjunto de reglas que realiza la comunicación de datos a través de una red a fin de llevar a cabo diferentes transacciones. Por ejemplo, el Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP) define un conjunto de reglas que se utilizan en el envío de datos de un nodo a otro de la red. El Protocolo Simple de Transferencia de Correo (SMTP) es un conjunto de reglas y estándares que se utilizan para la transferencia de correo electrónico y archivos adjuntos de un nodo a otro. El Protocolo dinámico de configuración de anfitrión (DHCP) es un protocolo —un conjunto de reglas y estándares— que se utiliza para asignar, de manera dinámica, direcciones IP en una red, a fin de que no sea necesario asignarlas a cada estación de trabajo en forma manual.

En la conectividad de redes se utilizan muchos protocolos. En realidad, en cierto sentido, *casi* todas las actividades en una red están regidas por un protocolo de un tipo o de otro. Algunos protocolos funcionan en niveles bajos del modelo de red OSI, otros trabajan en niveles altos y algunos más trabajan entre éstos.

En este capítulo usted aprenderá acerca de los protocolos de conectividad de redes utilizados para transmitir y recibir datos a través de una red.

COMPRENSIÓN DE TCP Y UDP

Como su nombre lo sugiere, TCP/IP son en realidad dos protocolos que se utilizan en concierto uno con el otro. El *Protocolo Internet (IP)* define cómo se direccionan los datos de la red desde una fuente hacia un destino y qué secuencia de datos debe reensamblarse en el otro extremo. El protocolo IP trabaja en la capa de red del modelo OSI. El *Protocolo de control de la transmisión (TCP)* es un protocolo de alto nivel que trabaja una capa más arriba que el IP, en la capa de transporte. TCP administra las conexiones entre computadoras. Los mensajes TCP son transportados (encapsulados) en datagramas IP.

El *Protocolo de datagrama de usuario (UDP)* sirve para el mismo propósito que TCP, pero ofrece un menor número de características. Tanto los paquetes TCP como los UDP son transportados dentro de paquetes IP, pero la única característica de confiabilidad que soporta UDP es el reenvío de cualquier número de paquetes que no se reciban en el destino. (El protocolo UDP es *no orientado a la conexión*.) La ventaja primordial del UDP es que es más rápido en comu-

¡DEFÍNALO! Datagramas, tramas y paquetes

Un *paquete* es cualquier grupo de datos enviados a través de una red. Usualmente, el término se utiliza, de manera genérica, para referirse a unidades de datos enviados por cualquier capa del modelo OSI. (Así que, por ejemplo, la gente habla acerca de los *paquetes IP*, a pesar de que técnicamente el término correcto es *datagramas IP*. En este libro, *paquete* se utiliza de forma genérica. La definición elegante de paquete se aplica solo a los mensajes enviados por la capa superior del modelo OSI, la capa de aplicación). Las unidades de datos de la capa de red, como las que transporta el protocolo IP, se llaman *datagramas*, mientras que las unidades de datos que transporta la capa de enlace de datos (capa uno) se llaman *tramas*. Todos éstos son solo términos que se refieren a un grupo de datos que se transmiten como una sola unidad.

nicaciones de red triviales, como el envío de páginas web a una computadora cliente. Debido a que UDP no ofrece muchas características en cuanto a la verificación y manejo de errores, debe utilizarse solo cuando no sea muy importante que los datos ocasionalmente se congestionen entre dos puntos, o cuando un programa de aplicación ofrezca sus propias funciones de verificación y manejo de errores.

Puertos TCP y UDP

Tanto TCP como UDP soportan el concepto de *puertos*, o de direcciones específicas de aplicación, con la ayuda de las cuales los paquetes se envían a cualquier máquina receptora. Por ejemplo, la mayoría de los servidores web corren en una computadora tipo servidor y reciben paquetes a través del puerto número 80. Cuando una máquina recibe un paquete que está destinado al servidor web (como una solicitud de una página web), la computadora que lo solicita envía esos paquetes al puerto con ese número. Cuando usted solicita una página web del servidor, su computadora envía la solicitud a la computadora servidora y especifica que su solicitud debe enviarse al puerto 80, que es adonde se envían las solicitudes HTTP. Cientos de puertos diferentes tienen usos estandarizados y es fácil definir sus propios puertos en un servidor para aplicaciones específicas. Un archivo de texto llamado SERVICES define los puertos de una computadora. A continuación se muestra un ejemplo de una parte del archivo SERVICES de Windows NT. (Solo se muestran algunas instrucciones debido a las restricciones de espacio; lo que sigue no es el archivo SERVICES completo, pero ilustra el contenido del mismo).

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This file contains port numbers for well-known
# services as defined by
# RFC 1700 (Assigned Numbers).
#
# Format:
#
# <service name><port number>/<protocol>[aliases...][#<comment>]
#
echo                 7/tcp
echo                 7/udp
discard              9/tcp    sink null
discard              9/udp    sink null
systat              11/tcp    users            #Active users
daytime             13/tcp
daytime             13/udp
chargen             19/tcp    ttytst source    #Character generator
chargen             19/udp    ttytst source    #Character generator
ftp-data            20/tcp                     #FTP, data
ftp                 21/tcp                     #FTP. control
telnet              23/tcp
smtp                25/tcp    mail             #SMTP
time                37/tcp    timserver
time                37/udp    timserver
```

```
tftp                69/udp                        #Trivial File Transfer
gopher              70/tcp
finger              79/tcp
http                80/tcp    www www-http        #World Wide Web
kerberos-sec        88/tcp    krb5                #Kerberos
kerberos-sec        88/udp    krb5                #Kerberos
rtelnet            107/tcp                        #Remote Telnet Service
pop2               109/tcp    postoffice          #POP-V2
pop3               110/tcp                        #POP v3-
nntp               119/tcp    usenet              #NNTP
ntp                123/udp                        #Network Time Protocol
snmp               161/udp                        #SNMP
snmptrap           162/udp    snmp-trap           #SNMP trap
print-srv          170/tcp                        #Network PostScript
irc                194/tcp                        #Relay Chat Prot
ipx                213/udp                        #IPX over IP
ldap               389/tcp                        #Lightweight DAP
https              443/tcp    MCom
https              443/udp    MCom
who                513/udp    whod
cmd                514/tcp    shell
syslog             514/udp
printer            515/tcp    spooler
router             520/udp    route routed
netnews            532/tcp    readnews
uucp               540/tcp    uucpd
wins              1512/tcp                        #Windows Name Service
```

Como usted podrá observar, la mayoría de los servicios de Internet con los que está familiarizado en realidad trabajan por medio del uso de los puertos TCP y/o UDP, como HTTP para la web, SMTP para correo electrónico, NNTP para Usenet, etc. El uso de puertos asegura que las comunicaciones de red que se desean utilizar para un propósito en particular no se confundan con otras que puedan estar llegando a la misma máquina. Los puertos permiten que la máquina receptora envíe, adecuadamente, los datos que están llegando a ella. Un ejemplo es un servidor que almacena páginas web y también recibe y procesa correo electrónico. Los paquetes que llegan al puerto 80 se enviarán al software servidor de red, mientras que los que lleguen al puerto 25 se enviarán al software de correo electrónico. Otros servicios de la máquina como Telnet y FTTP, también pueden funcionar de manera concurrente mediante este mecanismo.

Paquetes IP y direccionamiento IP

En los paquetes IP se incluyen direcciones que definen, de manera única, cada computadora conectada a Internet (consulte la figura 8-1). Estas direcciones se utilizan para enrutar paquetes de un nodo emisor a uno receptor. Debido a que todas los ruteadores de Internet conocen las direcciones de red a las que están conectados, pueden enviar paquetes, de manera muy precisa, que tengan como destino una red remota.

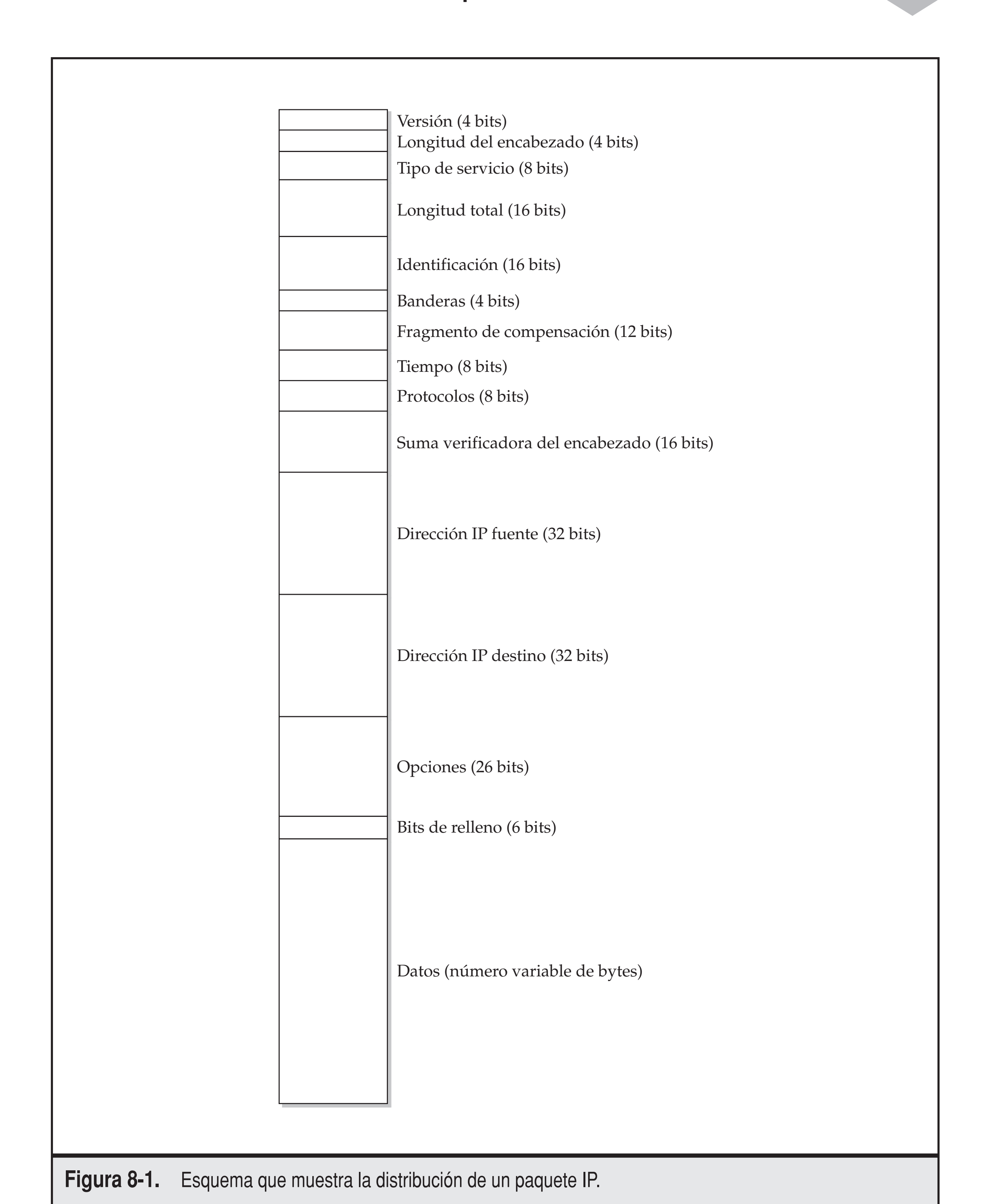


Figura 8-1. Esquema que muestra la distribución de un paquete IP.

Además de transportar sus datos, cada paquete IP contiene varios campos. Estos campos, en el orden en el que se encuentran, son:

- **Versión** Ésta es la versión del protocolo IP que se está utilizando. Indica, por ejemplo, si se está utilizando la versión 4 o la versión 6 de IP.
- **Longitud del encabezado** Este campo indica la longitud de la información del encabezado antes de que comiencen los datos que contiene el paquete.
- **Tipo de servicio** Este campo es utilizado para diferentes actividades por los diversos fabricantes. Puede utilizarse para funciones como solicitud de enrutamiento de alta prioridad, solicitud de envío con el más alto nivel de confiabilidad, etcétera.
- **Longitud total** Este campo indica la longitud total del paquete.
- **Identificación, banderas y fragmentos fuera de su lugar** Estos tres campos se utilizan para reensamblar cualquier paquete IP que haya sido desensamblado en algún punto durante la transmisión. Estos campos incluyen toda la información necesaria para reensamblar correctamente los paquetes en el extremo receptor.
- **Tiempo de vida** Este campo define cuántos saltos en la red puede realizar un paquete antes de que se le declare como muerto y los ruteadores dejen de enviarlo a otros ruteadores. Este número se establece cuando se envía el paquete y cada ruteador que lo maneja decrementa dicho número una unidad. Cuando el número llega a un valor de cero, el paquete se considera muerto y ya no es transmitido.
- **Protocolo** Este campo indica si el paquete IP está contenido en un paquete TCP o UDP.
- **Suma de verificación del encabezado** La suma verificadora del encabezado se utiliza para asegurarse de que ningún dato (los campos estudiados en esta lista) del encabezado del paquete resulte dañado.
- **Dirección IP fuente** Este campo contiene la dirección de la computadora emisora, la cual es necesaria cuando un paquete debe ser retransmitido, en cuyo caso el nodo receptor (o, en algunos casos, un ruteador) conoce a qué nodo solicitar una retransmisión.
- **Dirección IP destino** Este campo contiene la dirección del nodo receptor.
- **Opciones y relleno** Estos dos campos finales del encabezado del paquete IP se utilizan para solicitar cualquier instrucción acerca de algún enrutamiento específico que se requiera o para especificar el tiempo en el que se envió el paquete.
- **Datos** El campo final de un paquete IP son los datos que, en realidad, están siendo enviados.

Las direcciones IP son de 32 bits de longitud, lo que permite que el número máximo de direcciones sea de 2E32 o aproximadamente 4.3 mil millones de direcciones. Para que sea más fácil trabajar con ellas y para enrutarlas de una manera más eficiente, se dividen en cuatro *octetos*, cada uno con una longitud de un byte. Por tanto, en notación decimal, las direcciones IP se expresan como *xxx.xxx.xxx.xxx*, donde cada *xxx* representa un número de 0 a 255. Los números 0, 127 y 255 están generalmente reservados para propósitos especiales, por lo que típicamente no se encuen-

¡Ayuda! ¡Se están acabando las direcciones!

La implantación actual de IP, llamada versión 4 de IP (IPv4), avanza hacia el punto en el que se está convirtiendo en una posibilidad real que se agoten las direcciones. En 1994 se generó una propuesta para vencer esta limitación. Llamada próxima generación IP (IPng y ahora IPv6), la nueva versión de IP atiende esta limitante de direccionamiento mediante el aumento de la longitud de las direcciones de 32 bits a 128 bits. Ello permite tener 3.4 × 10 E 38 (un 34 seguido por 37 ceros, o cerca de 340 trillones de trillones de trillones) direcciones únicas, que deben dejar un espacio lo suficientemente grande para todas las direcciones de Internet que surjan en el futuro, lo cual permite que ¡incluso los refrigeradores, los tostadores y los automóviles tengan sus propias direcciones IP!

tran disponibles para los nodos, mientras que las 253 direcciones restantes están disponibles para asignarse en cada octeto.

Se garantiza que las direcciones en Internet sean únicas por medio del uso de un servicio de registro de direcciones, que actualmente se encuentra administrado por la Corporación de Internet para la Asignación de Nombres y Números (ICANN). En realidad, los registros de los nombres y las direcciones de dominio están administrados mediante uno de los tantos *registradores*, los cuales incluyen compañías como INTERNIC, Network Solutions y muchas otras. El ICANN representa la autoridad máxima.

El ICANN asigna tres clases principales de direcciones, llamadas A, B y C. Para una dirección clase A, el ICANN asigna al propietario un número en el primer octeto; el propietario es libre de utilizar todas las combinaciones posibles de los tres octetos restantes. Por ejemplo, una dirección clase A podría ser 57.*xxx.xxx.xxx*. Las direcciones clase A permiten que el propietario asigne direcciones hasta 16.5 M nodos únicos. Las direcciones clase B definen los dos primeros octetos y deja los dos restantes libres para el uso del propietario de las direcciones. Por ejemplo, 223.55.*xxx.xxx* podría ser una asignación de dirección clase B válida. Las direcciones de esta clase permiten que el propietario tenga 65 K nodos únicos. Las clase C siguen esta progresión, es decir, definen los primeros tres octetos y dejan solo el último octeto disponible para que sea asignado por el propietario de la clase C, lo cual permite que el propietario asigne hasta 255 nodos únicos.

Un proveedor del servicio de Internet (ISP) podría ser propietario de direcciones clase A o clase B, y después podría manejar varias direcciones clase C dentro de su propia estructura de direcciones. Cambiar de ISP, aun para una compañía que tenga una dirección clase C válida, significa un cambio en la dirección de la compañía de una dirección clase C disponible a través del primer ISP a una dirección clase C disponible de un segundo ISP.

Como se mencionó antes, las direcciones 0, 127 y 255 están reservadas. En general, la dirección 0, como la 123.65.101.0, se refiere a la red en sí, por lo cual el ruteador que conecta la red con las demás redes maneja esta dirección. La dirección 127 es una *dirección especial de retroalimentación* que puede utilizarse para cierto tipo de pruebas. La dirección 255 se refiere a todas las computadoras de la red, por lo que un mensaje difundido a la dirección 223.65.101.255 iría a todas las direcciones que estuvieran en 223.65.101.*xxx*.

Subredes IP

Las direcciones IP están formadas por dos componentes principales. El primero —el de la izquierda— es la *ID de red*, también llamada *netid*. El otro es el *host ID*, generalmente escrito sin el espacio como *hostid*. La netid identifica la red, mientras que el hostid identifica cada nodo de esa red. (Recuerde que en el argot de IP, todos los nodos se llaman *host* sin tomar en cuenta si es un servidor, una computadora cliente, una impresora o lo que sea).

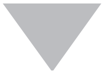
Para una dirección clase C, por ejemplo, la netid se coloca en los primeros tres octetos, mientras que el hostid utiliza el cuarto octeto. Para una dirección clase B, los primeros dos octetos son la netid, mientras que los dos octetos finales son hostids.

Para comprender cómo funcionan las subredes, considere una compañía que tenga tres redes en tres edificios diferentes, todas conectadas a través de un enlace ISDN de 64 Kbps. Cada red tiene aproximadamente 25 nodos. Cada edificio tiene su propio conjunto de servidores e impresoras para los trabajadores de ese edificio. El enlace ISDN entre las redes es para el caso de que sea necesario transmitir información entre los edificios, como mensajes de correo electrónico o transacciones contables. ¿Cómo asignaría la compañía direcciones IP en esta situación?

Una posibilidad sería que solicitara un solo conjunto de direcciones clase C y después las asignara a las tres redes de alguna manera. Esto parece ser una solución sencilla, pero es una idea muy pobre por un par de razones. Por lo general, mucho tráfico de la red se envía a cada hostid dentro de una sola netid. El enlace ISDN lento entre los edificios se convertiría verdaderamente en un cuello de botella en esta situación y toda la red funcionaría muy pobremente.

Otra idea es utilizar direcciones clase C diferentes (netids) en cada edificio. Ésta es una solución relativamente sencilla y trabajaría muy bien, excepto que posiblemente el ISP no pueda asignar tres direcciones clase C separadas y sería un desperdicio terrible de las direcciones IP disponibles. En esta situación, cada edificio estaría desperdiciando más de 200 direcciones.

¿Qué pasaría si hubiera una forma de dividir una dirección clase C de forma que cada edificio pudiera tener su propia netid virtual? Dicha solución es de lo que trata la subred. La subred permite subdividir una netid (generalmente la dirección clase C, pero dicha subred puede también hacerse con direcciones clase A o C) en dos o más redes.



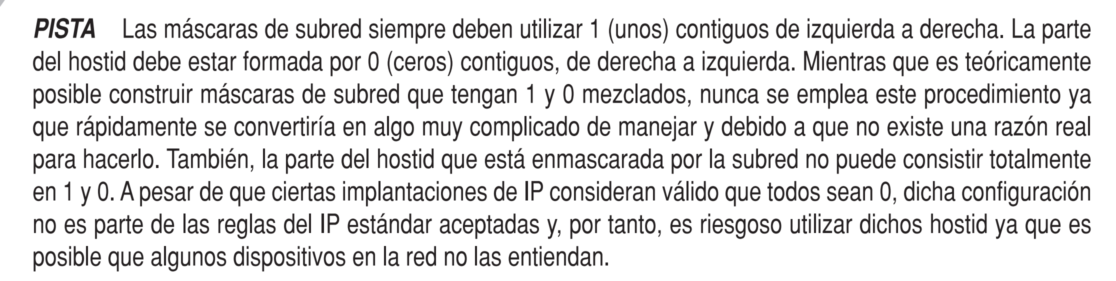
PISTA Para entender la subred, usted tiene que entender primero la representación binaria de las direcciones IP. Para obtener un panorama general de cómo se manejan los números binarios, consulte el capítulo 2.

Máscaras de subred

Si usted observa la configuración IP de una computadora, podrá ver que ésta siempre tiene tanto una dirección IP (como 205.143.60.109) como una *máscara de subred* (como 255.255.255.0). Es la máscara de subred la que define qué parte de la dirección IP de la computadora es la netid y cuál el hostid. Para ver esto de una manera más clara, usted necesita representar las direcciones en forma binaria.

Computer IP Address (Dec):	205	143	60	109
Computer IP Address (Bin):	11001101	10001111	00111100	01101101
Subnet mask (Dec):	255	255	255	0
Subnet mask (Bin):	11111111	11111111	11111111	00000000

La netid de una dirección, definida por la máscara de subred, es cualquier parte de la dirección que tenga un número binario 1 fijado en la máscara de subred correspondiente. En el ejemplo anterior, la netid está formada por los primeros tres octetos en su totalidad (los primeros 24 bits), y el hostid es el último octeto (los 8 últimos bits). Ahora puede ver por qué el 255 (decimal) se utiliza con tanta frecuencia en las máscaras de subred: es debido a que el 255 corresponde a tener todos los bits fijos al valor 1 en un número de 8 bits.



PISTA Las máscaras de subred siempre deben utilizar 1 (unos) contiguos de izquierda a derecha. La parte del hostid debe estar formada por 0 (ceros) contiguos, de derecha a izquierda. Mientras que es teóricamente posible construir máscaras de subred que tengan 1 y 0 mezclados, nunca se emplea este procedimiento ya que rápidamente se convertiría en algo muy complicado de manejar y debido a que no existe una razón real para hacerlo. También, la parte del hostid que está enmascarada por la subred no puede consistir totalmente en 1 y 0. A pesar de que ciertas implantaciones de IP consideran válido que todos sean 0, dicha configuración no es parte de las reglas del IP estándar aceptadas y, por tanto, es riesgoso utilizar dichos hostid ya que es posible que algunos dispositivos en la red no las entiendan.

Regresemos al ejemplo anterior de una compañía con tres edificios. ¿Qué sucedería si la compañía pudiera dividir una sola dirección clase C de forma que cada edificio pudiera utilizar su propia parte, y los ruteadores que conectan los edificios comprendieran cuáles envíos deberán mandarse a los otros edificios y cuáles no? En configuraciones como ésta es donde son de utilidad las máscaras de subred. Una máscara de subred le permite "tomar prestados" algunos bits de sus hostids y después utilizarlos para crear nuevas netids. Para el ejemplo que se mostró, usted necesitará tomar prestados tres bits de la dirección clase C (el cuarto octeto) y utilizar esa dirección para crear cuatro netids separados. Analice cómo trabajaría esta configuración en formato binario:

Subnet mask (Bin):	11111111	11111111	11111111	**111**00000
Bldg. 1 IP addresses:	11001101	10001111	00111100	**100**xxxxx
Bldg. 2 IP addresses:	11001101	10001111	00111100	**011**xxxxx
Bldg. 3 IP addresses:	11001101	10001111	00111100	**101**xxxxx
Subnet mask (Dec):	255	255	255	224
Bldg. 1 IP addresses:	205	143	60	129 – 158
Bldg. 2 IP addresses:	205	143	60	97 – 126
Bldg. 3 IP addresses:	205	143	60	161 – 190

El ejemplo anterior toma tres bits del rango de direcciones clase C de la compañía y después usa este rango de direcciones para crear 6 netids que la compañía puede utilizar, con lo cual se ofrece a cada edificio 30 direcciones de hostid posibles. Utilizando subredes para asignar cada netid por separado, la compañía puede programar los ruteadores para enviar paquetes entre las redes solo cuando los paquetes tengan que ser enrutados, y no de otra forma.

Máscara binaria	Equivalente decimal	Número de subredes	Número de hostids por subred
00000000	0	1	254
10000000	128	N/A	N/A
11000000	192	2	62
11100000	224	6	30
11110000	240	14	14
11111000	248	30	6
11111100	252	62	2
11111110	254	N/A	N/A
11111111	255	N/A	N/A

Tabla 8-1. Máscaras de subred más comunes.

Debido a que las máscaras de subred usualmente se crean utilizando bits contiguos para la máscara en sí, solo nueve máscaras de subred se usan con frecuencia, como se muestra en la tabla 8-1.

Observe en la tabla 8-1 que algunas configuraciones están marcadas como "N/A" (no se aplica). Estas máscaras de subred darían como resultado que no hubiera direcciones disponibles, debido a la regla de que la parte de subred de la netid no puede estar formada totalmente por 0 ó 1. Por ejemplo, considere la máscara de subred del 224, la cual utiliza tres bits de hostid en la subred. En teoría, esta configuración generaría ocho subredes. Sin embargo, las subredes representadas por 000 y 111 no son válidas, por lo que se pierden. De la misma forma, 128 no es una máscara de subred válida debido a que ese bit sería *siempre* 1 ó 0.



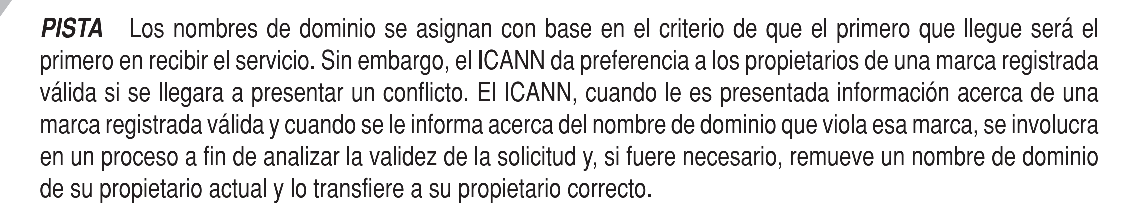
PISTA A medida que aprenda acerca de conectividad de redes con TCP/IP, es importante que usted comprenda cómo trabajan las subredes y los propósitos para los que se utilizan. Sin embargo, si necesita implantar subredes, debería inicialmente trabajar en este proyecto con un ingeniero en redes con experiencia, el que podrá ayudarlo a evitar muchos problemas que no se encuentran descritos explícitamente o que no se muestran en la sección anterior. También es probable que desee buscar un conocimiento más detallado acerca de TCP/IP. Se encuentran disponibles muchos libros que se dedican a este tema y lo estudian con mayor profundidad.

COMPRENSIÓN DE OTROS PROTOCOLOS DE INTERNET

En Internet se utilizan muy pocos protocolos que dependan, o hagan uso de TCP/IP. En esta sección usted aprenderá acerca de estos diferentes protocolos, lo que hacen y, cuando sea apropiado, cómo funcionan.

Sistema de nombres de dominio

Si todo lo que usted tuviera que usar para asignar direcciones a las computadoras en Internet fueran los números de dirección, tratar de guardar un record de ellos y utilizar las direcciones correctas de red lo volvería loco. Por ejemplo, para ir al sitio web de Yahoo!, tendría que recordar teclear la dirección **http://204.71.202.160**. Para resolver este problema, se desarrolló un sistema llamado Sistema de Nombres de Dominios (DNS). Este sistema permite que la gente registre números de dominio con ICANN y, después, los utilice para acceder a un nodo en particular en Internet. Por tanto, DNS es el servicio que le permite abrir un navegador web y teclear **http://www.yahoo.com** y, después, conectarse a una computadora particular a través de Internet. En este caso, **yahoo.com** es el nombre completo del dominio.



PISTA Los nombres de dominio se asignan con base en el criterio de que el primero que llegue será el primero en recibir el servicio. Sin embargo, el ICANN da preferencia a los propietarios de una marca registrada válida si se llegara a presentar un conflicto. El ICANN, cuando le es presentada información acerca de una marca registrada válida y cuando se le informa acerca del nombre de dominio que viola esa marca, se involucra en un proceso a fin de analizar la validez de la solicitud y, si fuere necesario, remueve un nombre de dominio de su propietario actual y lo transfiere a su propietario correcto.

Los dominios se encuentran organizados en tres arreglos, como el árbol de direcciones de un disco duro. En el nivel más alto se definen diferentes *tipos de dominio*, llamados *nombre de dominio de alto nivel (TLD)*. El tipo de dominio más común es el .com, el cual se utiliza generalmente para entidades comerciales con fines de lucro. Otros tipos de dominio muy comunes son los siguientes.

- .edu, para instituciones educativas
- .gov, para entidades gubernamentales
- .mil, para entidades militares
- .net, para entidades relacionadas con Internet
- .org, para entidades no lucrativas
- .xx, para los diferentes países —por ejemplo, **.it** para Italia, **.de** para Alemania, etcétera.

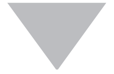
NOTA En años recientes se han adicionado muchos TLD al sistema, como .biz, .info, .name y otras. Usted podrá encontrar una lista completa de TLD´s en **http://www.icann.org**.

Dentro de un nombre de dominio, las entidades son libres de incluir otros nombres antes del comienzo del nombre de dominio, los cuales, generalmente, se refieren a un host o servidor en particular o, a veces, a un tipo particular de servicio para ese dominio. Por ejemplo, si usted tiene el dominio **bedrock.gov**, estaría en todo su libertad para crear nombres adicionales, como **quarry.bedrock.gov** o **flintstone.bedrock.gov**.

Como algo propio de los estándares, la primera parte del nombre de un dominio que le precede al nombre del dominio real indica a qué tipo de servicio se está conectando. Por ejemplo, **www.bedrock.gov** se utilizaría para un servidor en la telaraña de la información (World Wide

Web) para el dominio **bedrock.gov**, mientras que **ftp.bedrock.gov** se utilizaría para un servidor FTP, etc. Los estándares de los tipos de servicio dentro del nombre de dominio están generalmente seguidos, pero no siempre. El propietario del nombre del dominio tiene toda la libertad de inventar sus propios tipos de servicio que le satisfagan alguna necesidad. Por ejemplo, algunos propietarios de nombres de dominio se refieren a sus servidores de correo electrónico como **smtp.domain.org**, mientras que otros preferirían utilizar **mail.domain.org**. Los propietarios podrían también utilizar cualquier otro nombre que les plazca.

Los nombres de dominio se convierten en direcciones IP mediante el uso de servidores de *nombres de dominio* (servidores DNS), los cuales aceptan el nombre del dominio tecleado, que llevan a cabo una consulta en bases de datos, y después regresan la dirección real que debe utilizarse en ese nombre de dominio. En general, cada ISP le da mantenimiento a sus propios servidores DNS (y muchas compañías y organizaciones también le dan mantenimiento a sus propios servidores DNS). Cualquier cambio se propaga a través de todos los servidores DNS de Internet, por un espacio de una hora aproximadamente.



NOTA Los cambios de parámetros del DNS solían tomar algunos días en propagarse a través de Internet, pero las modificaciones que se le han introducido al sistema permiten que se propaguen más rápido, a menudo solo minutos después de que se generan.

Protocolo dinámico de configuración del host (DHCP)

En los primeros días de las redes basadas en TCP/IP, los administradores definieron cada dirección de red en un archivo de texto o caja de diálogo. De ahí en adelante, la dirección era fija, a menos que alguna persona la cambiara. El problema fue que los administradores ocasionalmente podrían, por error, definir direcciones conflictivas en otros nodos de la red, lo cual provocaría un verdadero caos. Para resolver este problema y facilitar la asignación de direcciones TCP/IP, se inventó un servicio llamado Protocolo Dinámico de Configuración del Host (DHCP).

Los servicios del DHCP corren en un servidor DHCP, donde controlan un rango de direcciones IP llamadas *objeto*. Cuando los nodos se conectan a la red, contactan al servidor DHCP para obtener una dirección asignada que puedan utilizar. Se dice que las direcciones de un servidor DHCP se le rentan al cliente que las usa, con lo que se quiere dar a entender que se conservan asignadas a un nodo en particular por un periodo antes de que expiren y estén disponibles para que otro nodo las utilice. A menudo, los periodos de renta son de solo algunos días, pero los administradores de la red pueden establecer cualquier periodo que deseen.

¡DEFÍNALO! Host

Usted podría pensar que un *host* es un servidor y en algunos contextos de la conectividad de redes, estaría en lo correcto. Sin embargo, en el argot de los nombres y las direcciones de Internet, a cada computadora que tenga una dirección IP se le llama *host*, y por ende, el nombre Protocolo Dinámico de Configuración del Host. (Recordar que a cada computadora se le llama host es particularmente importante en los mundos de UNIX y LINUX, donde el término es mucho más común que en los mundos de Windows y Macintosh).

Usted no debe utilizar DHCP en los nodos que ofrecen servicios de red, particularmente en servidores que proporcionan servicios a través de Internet. Ello se debe a que la modificación de una dirección TCP/IP haría imposible la conexión confiable a esas computadoras. En lugar de lo anterior, utilice DHCP para dar soporte a las estaciones de trabajo del cliente que no necesiten hospedar servicios para otros nodos.

Protocolo de transferencia de hipertexto (HTTP)

La telaraña mundial de la información está formada por documentos que utilizan un lenguaje de formateo llamado *HTML*, que significa Lenguaje de Marcado de Hipertexto. Estos documentos están compuestos por texto desplegable, imágenes gráficas, comandos de formateo e hiperenlaces a otros documentos ubicados en algún lugar de la web. La mayoría de las veces los documentos HTML se despliegan utilizando navegadores de la web, como Netscape Navigator o Internet Explorer, de Microsoft.

El protocolo llamado *Protocolo de Transferencia de Hipertexto (HTTP)* controla las transacciones entre un cliente de la web y un servidor de la web. HTTP es un protocolo de la capa de aplicación. El protocolo HTTP hace uso, en forma transparente, de DNS y otros protocolos de Internet para formar conexiones entre el cliente y el servidor de la web, de forma que el usuario esté consciente solo del nombre de dominio del sitio web y del nombre del documento.

HTTP es, básicamente, un protocolo inseguro. La información basada en texto se envía "tal cual" entre el cliente y el servidor. Para satisfacer la necesidad de conectividad confiable a la web, existen varias alternativas, como HTTP (S-HTTP) o Capa de los sockets seguros (SSL).

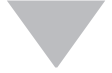
Las solicitudes de un cliente a un servidor web son orientadas a la conexión, pero no son persistentes. Una vez que el cliente recibe el contenido de una página HTML, la conexión ya no está activa. Si se teclea un hiperenlace en el documento HTML se reactiva el enlace, tanto del servidor original (si es hacia donde apunta el hiperenlace), como de otro servidor en algún otro lado.

Protocolo de transferencia de archivos (FTP)

Las siglas *FTP* significan dos cosas: Protocolo de Transferencia de Archivos y Programa para la Transferencia de Archivos (el cual hace uso del Protocolo de Transferencia de Archivos). Es algo como, "it´s a dessert topping *and* a floor polish" del programa de televisión *Saturday Night Live*. Debido a que FTP (el programa) utiliza FTP (el protocolo), es posible que sea confuso saber de cuál se está hablando. En esta sección se estudia este protocolo. (Cuando me refiera al programa, lo aclararé).

FTP es un protocolo de la capa de aplicación que se utiliza para enviar y recibir archivos entre un cliente FTP y un servidor FTP. Generalmente, esta operación se lleva a cabo con el programa FTP u otro que también pueda utilizar el protocolo (existen muchos disponibles). Las transferencias por FTP pueden estar basadas en texto o en lenguaje binario y pueden manejar archivos de cualquier tamaño. Cuando usted se conecta a un servidor FTP para transferir un archivo, ingresa al servidor FTP utilizando un nombre de usuario y una contraseña válidos. Sin embargo, muchos sitios están considerados para permitir algo que se llama *FTP anónimo*, donde usted ingresa el nombre anónimo del usuario y después ingresa su dirección de correo electrónico como contraseña. Por ejemplo, Microsoft mantiene un sitio FTP que puede utilizar para bajar actualizaciones de sus productos. Está ubicado en **ftp.microsoft.com**, y es un ejemplo de un sitio que permite FTP anónimo.

Para utilizar el programa FTP, en la mayoría de las plataformas, usted teclea el comando **ftp** seguido de la dirección a la que se desea conectar. Así que, para utilizar el ejemplo de Microsoft, usted teclearía **ftp.microsoft.com** y, después teclearía ENTER. Después ingresaría al sistema y podría utilizar todos los comandos FTP, esto es, PUT, GET, MGET, etc. La mayoría de las implantaciones cuentan con ayuda en línea a fin de proporcionarle información acerca de los diferentes comandos. Presione la tecla ? o HELP para poder acceder a esta facilidad.



PISTA Versiones recientes de Windows también soportan conexiones FTP utilizando Internet Explorer. Solo abra el Explorador y en lugar de ingresar una dirección **http:**// en la barra de direcciones, teclee una dirección precedida por **ftp:**//. Por ejemplo, para conectarse al servidor FTP de Microsoft, usted debe utilizar la dirección **ftp:**//**ftp.microsoft.com**. Este truco también funciona con la mayoría de los otros navegadores de la web, como Mozila Firefox. Observe que en los sitios ftp que requieren una clave de acceso, el navegador debe soportar el ingreso. En Internet Explorer, existe un comando Logon As en el menú File después de que trate de navegar en dicho sitio ftp.

Protocolo de transferencia Netnews (NNTP)

Usenet (NetNews) es un conjunto de grupos de estudio que se dedican a analizar una gran variedad de temas. Actualmente existen más de 35 000 de estos grupos. Las conversaciones de Usenet se colocan en servidores Usenet, los cuales difunden sus mensajes a todos los demás servidores del mismo tipo en todo el mundo. Un mensaje colocado puede viajar a través de todos los servidores Usenet en cuestión de horas y después estar disponible para los usuarios que accedan a cualquier servidor de éstos en particular.

Los grupos de estudio de Usenet están organizados como las ramas de un árbol. Las siguientes son algunas de las ramas principales:

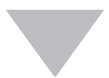
- **Alt,** utilizado en el estudio acerca de estilos de vida alternos y otros temas misceláneos.
- **Comp,** utilizados en estudios orientados a la computadora.
- **Gov,** en análisis orientados al gobierno.
- **Rec,** dedicados a temas acerca de recreación.
- **Sci,** dedicados a estudios relacionados con la ciencia.

Los grupos Usenet pueden ser públicos, los cuales son difundidos a otros servidores de Usenet, o privados, los cuales son generalmente patrocinados por una organización en particular y requiere que el usuario ingrese sus credenciales de acceso antes de poder leer y colocar mensajes.

El protocolo NNTP es lo que hace posible NNTP. Permite la conexión entre un lector de Usenet (también llamado *lector de noticias*) y un servidor Usenet. Asimismo, ofrece el formateo de mensajes, por lo que los mensajes pueden estar basados en texto o también contener adjuntos binarios. Los adjuntos binarios en envíos a través de Usenet están normalmente codificados utilizando la Codificación de Mensajes de Internet Multipropósito (MIME), la cual se utiliza también para mensajes adjuntos de correo electrónico. Sin embargo, algunos sistemas más antiguos emplean métodos diferentes para codificar adjuntos, entre ellos otro método llamado UUEncode/UUDecode y, en la Macintosh, un método llamado BinHex.

Telnet

Telnet define un protocolo que permite que se establezca una sesión terminal remota con un host Internet, para que así los usuarios remotos tengan acceso similar al que tendrían si estuvieran sentados en una terminal conectada a la computadora host. Mediante Telnet los usuarios pueden controlar el host remoto y llevar a cabo tareas como la administración de archivos, correr aplicaciones o incluso (con los permisos apropiados), administrar el sistema remoto.



NOTA Telnet es un protocolo de la capa de sesión del modelo OSI.

Para que Telnet trabaje, el software de Telnet debe estar corriendo tanto en el servidor como en la computadora del cliente. Usted debe correr el programa Telnet en una computadora cliente y el programa Telnet en la computadora del servidor para permitir la conexión. Telnet es específico del protocolo TCP y por lo general corre en el puerto 23 (aunque puede correr en cualquier otro puerto que haya sido habilitado en el sistema servidor). Una vez que los usuarios se conecten mediante Telnet, deben ingresar al sistema remoto utilizando las mismas credenciales que se les requeriría si estuvieran utilizando una terminal conectada directamente.

Protocolo simple de transferencia de correo (SMTP)

El correo electrónico tuvo un comienzo espectacular, con programas anteriores de correo electrónico que compartían algunos estándares con otros programas similares, particularmente en el manejo de datos binarios adjuntos. La buena noticia es que la situación está resuelta ahora y todo el software de correo electrónico actual soporta todos los estándares que están aceptados ampliamente.

El Protocolo Simple de Transferencia de Correo (SMTP) se utiliza para enviar y recibir mensajes de correo electrónico de un servidor de correo electrónico a otro. Los detalles de SMTP pueden encontrarse en RFC 821. El protocolo SMTP define un diálogo entre un sistema emisor y uno receptor.

Un diálogo SMTP comienza cuando un sistema emisor se conecta al puerto 25 de un sistema receptor. Una vez que se establece la conexión, el sistema emisor envía un comando HELO, seguido de su dirección. El sistema receptor reconoce el comando HELO junto con su propia dirección. El diálogo, después, continúa cuando el sistema emisor genera un comando que indica que el sistema desea enviar un mensaje e identifica al receptor al que se dirige. Si el sistema receptor conoce el destino, éste reconoce la solicitud y, después, el sistema emisor transmite el cuerpo del mensaje junto con sus adjuntos. Por último, la conexión entre los dos sistemas se termina una vez que el sistema receptor reconoce que ha sido recibido todo el mensaje. La figura 8-2 ilustra este proceso.

Voz sobre IP (VoIP)

Un grupo importante de protocolos IP que está en sus comienzos trata acerca de la transmisión de información de voz y fax a través de las redes basadas en IP, llamadas *Voz sobre IP* o, en forma abreviada, *VoIP*. VoIP es un protocolo que permite que la voz analógica de llamadas telefónicas sea digitalizada y después encapsulada en paquetes IP transmitidos a través de una red. VoIP puede utilizarse para transportar llamadas telefónicas de voz a través de una red IP, como una LAN o WAN de una compañía o a través de Internet. Existen ventajas y desventajas

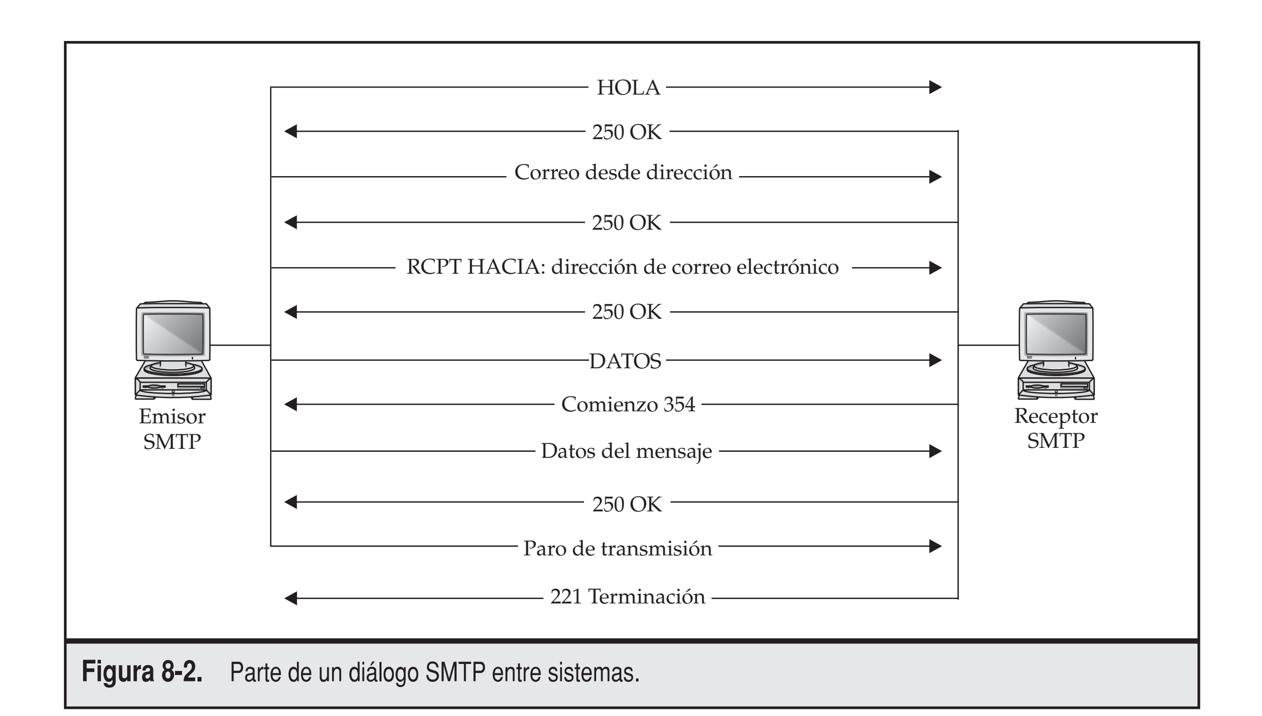


Figura 8-2. Parte de un diálogo SMTP entre sistemas.

importantes respecto al envío de tráfico de voz a través de una red utilizando un protocolo basado en paquetes como IP, en contraposición con las conexiones conmutadas que utiliza normalmente el sistema telefónico. Estas ventajas y desventajas se estudian con detalle en las secciones siguientes.

Ventajas de VoIP

El envío de datos de voz a través de redes IP tiene ventajas muy atractivas.

Uso más eficiente de las conexiones disponibles Considere una compañía grande con dos oficinas principales. En cualquier momento, cientos de conversaciones de voz pueden estar ocurriendo entre esas dos oficinas. Cada conexión de voz convencional consume una línea DS0, capaz de transportar hasta 56 Kbps de datos si la línea se fuera a utilizar en forma digital. En realidad, cada conversación no utiliza todo el ancho de banda disponible en la línea. Parcialmente, ello se debe a que la mayor parte de las conversaciones tiene un gran número de espacios de silencio: tiempo entre palabras u oraciones, tiempo donde un suscriptor deja de hablar y el otro comienza, etc. Además, la mayoría de las conversaciones, si se codificaron digitalmente, podrían estar comprimidas de forma significativa. Sume todo esto y es probable que cada conversación de voz utilice solo de un tercio a la mitad del ancho de banda disponible en un solo circuito DS0. Si usted fuera capaz de transportar todas estas conversaciones de voz en forma digital, se requeriría una cantidad menor de ancho de banda. En lugar de 100 líneas DS0 para 100 conversaciones, por ejemplo, las mismas conversaciones podrían utilizar de 25 a 33 líneas DS0 si estuvieran empacadas digi-

talmente. Sume todos los ahorros de dinero y podrá usted ver que muchas compañías pueden ahorrarse una cantidad significativa de dinero si utilizan VoIP.

Las conexiones VoIP están orientadas a paquetes Cuando el usuario efectúa una llamada, se forma una sola conexión entre el emisor y el receptor. Esta conexión es estática durante el transcurso de la llamada. Sin embargo, si la conversación se digitalizara y se enviara a través de una red orientada a paquetes, habría muchas trayectorias posibles para cada paquete y se presentaría mucha más redundancia de manera automática. Por ejemplo, si alguna parte de la red entre los dos puntos fallara, los paquetes aún podrían llegar a su destino a través de una ruta alterna, de la misma forma en que los paquetes de datos lo hacen a través de Internet. Asimismo, los circuitos disponibles se utilizarían de una manera más eficiente, lo cual permitiría el enrutamiento de más llamadas dentro de un área geográfica en particular.

Desventajas de VoIP

Existen también algunos problemas con VoIP que usted necesita considerar.

No existe entrega garantizada VoIP no garantiza la entrega de paquetes IP a través de Internet. Esto no representa un gran problema en la transmisión digital de datos; si un paquete no se confirma como recibido, simplemente se retransmite. En el caso de una conversación de voz en tiempo real, por otro lado, la pérdida de paquetes inhibe la conversación de manera directa y no puede regresar en el tiempo para retransmitir los paquetes perdidos.

Los paquetes llegan fuera de secuencia No solo los paquetes IP pueden no llegar a su destino ocasionalmente, sino que a veces llegan fuera de secuencia debido la existencia de tráfico en Internet y a otras razones. Esto está bien para transmitir cosas como archivos, ya que éstos pueden ser reensamblados en el otro extremo con la secuencia correcta. Sin embargo, para una aplicación en tiempo real como la voz, tener paquetes que lleguen fuera de secuencia genera una confusión sin esperanzas y, por tanto, en una transmisión inútil.

QoS no está implantada ampliamente A las aplicaciones en tiempo real de Internet, como VoIP o multimedia y transmisiones sensibles al tiempo, se les debe dar prioridad sobre las transmisiones que no lo son en particular, como la transmisión de un mensaje de correo electrónico. Afortunadamente IP tiene un campo llamado calidad de servicio (QoS) que permite que el usuario asigne prioridades por dichas razones. Sin embargo, QoS no se ha implantado ampliamente en todas las partes de Internet.

Desarrollo y futuro de Internet

VoIP es una tecnología reciente muy prometedora que muy seguramente se convertirá en una parte importante de Internet y de la mayoría de las redes de las compañías. Sin embargo, aún hay mucho trabajo por hacer respecto de la implantación profunda de esta tecnología y la resolución de los problemas que se describen en esta sección. En otras palabras, si usted desea aprender acerca de conectividad de redes, deberá estar consciente de VoIP —qué es y qué hace—, aunque sea muy probable que la tecnología no se convierta en un factor importante en la mayoría de las redes hasta dentro de algunos años.

NOTA Existe un gran número de compañías que ofrecen servicios VoIP a clientes residenciales, dentro de las que se incluye a AT&T, Vonage, Verizon y Time Warner Cable. Estas compañías ofrecen paquetes que permiten un número de llamadas virtualmente ilimitado a través de una conexión de Internet existente de gran ancho de banda por un costo de 30 dólares adicionales al mes. Con frecuencia estas compañías ofrecen en un paquete el hardware de VoIP necesario cuando se contrata el servicio. La revista *Consumer Reports*, en su número de Febrero de 2005, proporciona un análisis de estos servicios y si usted puede conseguirlo, le recomiendo que lea el análisis y los comentarios.

COMPARACIÓN DE LOS PROTOCOLOS PROPIETARIOS IMPORTANTES

Mientras que las redes basadas en Microsoft, Novell y Apple pueden trabajar totalmente con TCP/IP y se analizaron previamente todos los protocolos, cada tipo de red comenzó soportando protocolos propietarios únicos de cada compañía y cada uno de ellos aún se usa mucho en la actualidad. Todas estas compañías han acogido a TCP/IP y lo soportan totalmente tanto en servidores como en clientes de red. En el caso de las redes Microsoft y Novell (desde que salió Windows NT 4 y Novell NetWare 5), pueden utilizarse fácilmente empleando solo TCP/IP. En teoría, usted podría hacer lo mismo con una red basada en Apple, pero perdería una gran cantidad de la funcionalidad que ofrece la red Macintosh si lo hiciera. Debido a lo anterior, una red basada en Apple debería soportar tanto a AppleTalk (protocolo propietario de Apple) como a TCP/IP.

Hasta muy recientemente, las redes Novell utilizaron predominantemente los protocolos de Intercambio de Paquetes de Red/Intercambio de Paquetes en Secuencia (IPX/SPX). Existen protocolos derivados del XNS de Xerox. A pesar de que es diferente de TCP/IP, IPX/SPX es compatible con ese protocolo; IPX es análogo a IP y SPX es análogo a TCP.

Originalmente, las redes Microsoft se basaban en un protocolo desarrollado por IBM llamado NetBIOS (*Sistema Básico de Entrada/Salida de Red*). NetBIOS es un protocolo de relativamente alto nivel que, en esencia, extiende la funcionalidad de DOS a una red. Microsoft también utilizó el NetBEUI (*Interfase de Usuario Extendida NetBIOS*) de IBM, una mejora de NetBIOS.

Las redes de computadoras Macintosh de Apple originalmente soportaban solo AppleTalk. El protocolo fue diseñado expresamente con el propósito de compartir las entonces caras impresoras LaserWriter, de Apple, dentro de pequeños grupos de trabajo utilizando una red de poco ancho de banda (230 Kbps originalmente) llamada LocalTalk. Con el tiempo, Apple mejoró AppleTalk para permitir la compartición de archivos y otras funciones de red, aún es un protocolo de red extremadamente ineficiente que, incluso sobre Ethernet (llamado EtherTalk en la implantación de Apple), trabaja muy lento. Aun así, si usted tiene un red basada en Apple, tiene que vivir con el protocolo AppleTalk.

IPX/SPX de Novell

El protocolo IPX de Novell fue originalmente una ramificación de la arquitectura de Sistemas de Red de Xerox (XNS) y se parece mucho a ésta. A pesar de que IPX puede utilizarse en cualquiera de las redes populares (Ethernet, Token Ring, etc.), fue diseñado originalmente para las redes Ethernet y trabaja muy bien con ese medio de transmisión. En realidad, el protocolo IPX depende de las direcciones MAC de Ethernet para parte de sus propias direcciones. Las direcciones de

IPX son dinámicas y se negocian automáticamente con el servidor en el momento de ingresar, en lugar de ser fijadas de manera estática, como es el caso de TCP/IP sin servicios DHCP. Una dirección de red de IPX comprende tanto una dirección de red de 32 bits como una dirección de nodo de 48 bits. Además, otros 16 bits se utilizan para un ID de conexión, lo cual permite hasta 65 000 conexiones exclusivas cliente/servidor entre un cliente y un servidor. El diseño de direcciones de IPX, en teoría, permite aproximadamente 281 trillones de nodos en cada una de las 16 millones de redes.

IPX fue originalmente diseñado solo para LAN, pero ha experimentado mejoras y ahora soporta conexiones WAN. A pesar de que por lo general es considerado un protocolo "parlanchín" que requiere un gran número de transacciones de envío/reconocimiento, IPX ha sido mejorado y ahora cuenta con una característica de modo ráfaga, que incrementa el tamaño de los paquetes destinados a una WAN y disminuye el número de comunicaciones hacia delante y hacia atrás que se requieren. El protocolo IPX es ruteable, pero solo si la red cuenta con un ruteador que maneje IPX.

Protocolos NetBIOS y NetBEUI

Originalmente IBM diseñó NetBIOS y NetBEUI para soportar redes pequeñas. Microsoft adoptó los protocolos como parte de LAN Manager, un sistema operativo de red construido sobre las versiones anteriores del sistema operativo OS/2.

Ninguno de los dos protocolos es ruteable; cada uno es apropiado para LAN pequeñas que no dependan de los ruteadores entre segmentos de LAN diferentes. Sin embargo, NetBIOS puede encapsularse dentro de paquetes TCP/IP en redes Windows NT mediante un servicio llamado NetBIOS sobre TCP/IP (abreviado como NBT, que quiere decir, NetBIOS sobre TCP/IP).

Las LAN de Microsoft (anteriores a Windows 2000) dependen de un servicio NetBIOS llamado Nombres de NetBIOS para identificar cada estación de trabajo de una manera única.

En una implantación simple de NetBIOS, los nombres están registrados en todas las estaciones de trabajo a través de un mensaje difundido. Si ninguna computadora se ha registrado con un nombre en particular, el registro del nombre tiene éxito. Sin embargo, en una red basada en Windows NT más compleja que también utilice TCP/IP, los nombres de NetBIOS se convierten en direcciones TCP/IP a través del uso del Servicio de Nombres de Internet de Windows (WINS). Los nombres también pueden convertirse mediante el empleo de parámetros estáticos de definición de nombres que se encuentran en un archivo llamado LMHOSTS (LAN Manager HOSTS). Debido a que muchas aplicaciones de conectividad de redes aún utilizan nombres NetBIOS, tanto WINS como LMHOSTS permiten que dichas aplicaciones sigan funcionando en una red que solo maneje el protocolo TCP/IP. En cuanto a la aplicación se refiere, aún funciona con NetBIOS, mientras que TCP/IP lleva a cabo el trabajo real tras bambalinas.

AppleTalk

AppleTalk se ha extendido en años recientes hacia AppleTalk Fase II, tecnología que permite ahora enrutar paquetes AppleTalk (suponiendo un ruteador con capacidad de manejar la versión Fase II). Esta versión puede correr sobre Ethernet, Token Ring o LocalTalk de Apple. Bajo Ethernet, AppleTalk utiliza una variante del tipo de trama 802.2 llamada Ethernet *SNAP* (*Punto de Acceso de Subred*).

No obstante que las computadoras Apple de Macintosh pueden utilizar tanto TCP/IP como IPX/SPX agregando un software especial, el sistema operativo de Macintosh depende de AppleTalk, por lo que ambos TCP/IP e IPX/SPX se traducen en cada nodo en mensajes AppleTalk antes de que sean transferidos al sistema operativo. Este proceso de traducción es una de las razones por las que Macintosh, de Apple, tiende a ser más lenta que otros tipos de computadoras sobre conexiones de red. Aun así, este método funciona y es relativamente fácil de configurar y mantener.

RESUMEN DEL CAPÍTULO

Este capítulo está cimentando en el conocimiento que usted obtuvo en los capítulos anteriores, por lo cual hace hincapié en los diferentes protocolos importantes involucrados en, virtualmente, todas las redes, entre ellas, Internet. Usted aprendió principalmente acerca del protocolo TCP/IP, el cual, en esencia, desplazó protocolos anteriores como IPX/SPX y NetBIOS/NetBEUI (aunque ambos todavía se utilizan). Usted también aprendió acerca de los protocolos de Internet específicos de la capa de aplicación, como SMTP, DHCP y HTTP. Estos protocolos son muy importantes para cualquier profesional involucrado en la conectividad de redes.

Sería muy deseable que los protocolos estudiados en este capítulo fuera todo con lo que tuviera que luchar, pero desafortunadamente, existen más protocolos que aprender. Algunos son específicos de ciertas funciones, como al acceso remoto a una red y se analizan en el capítulo correspondiente en este libro. Otros aún están siendo desarrollados y no son un factor ahora, pero pueden serlo en un futuro cercano. Como siempre, estar al tanto de la tecnología de las redes, si usted trabaja en este campo, es importante y estar actualizado en los protocolos que vayan surgiendo y que puedan ser importantes para cualquier tipo de red que usted administre o dé soporte, es muy valioso.

En el capítulo siguiente usted aprenderá acerca de los servicios de directorio: qué son, cómo funcionan, para qué son buenos y acerca del servicio de directorio principal que existe en la actualidad. Como usted aprenderá, un servicio de directorio es un servicio de red muy importante, sin el cual las redes más complejas serían más difíciles de utilizar y administrar.

CAPÍTULO 9

Servicios de directorio

En los comienzos de las LAN, la búsqueda de recursos del servidor fue muy simple. La mayoría de las organizaciones comenzaron con solo un servidor de archivo o dos, así que conocer qué archivos, impresoras y otros servicios estaban en qué lugares de la LAN era algo muy fácil.

En estos días, la situación es significativamente más compleja. Aun organizaciones relativamente pequeñas tienen múltiples servidores, cada uno de los cuales lleva a cabo tareas diferentes, pues almacenan grupos de archivos diversos, proporcionan servicios de Internet o intranet, conectan diferentes impresoras, etc.

Los servicios de directorio trabajan a fin de organizar todo este desorden. En este capítulo usted aprenderá qué hacen los servicios de directorio y cómo trabajan. También conocerá los servicios de directorio que se usan en la actualidad y los que se utilizarán en un futuro cercano. A medida que los servicios de directorio se conviertan en algo cada vez más importante para la administración de las redes, aprehender esta información se convertirá en una parte significativamente relevante del diseño, empleo y administración de redes.

¿QUÉ ES UN SERVICIO DE DIRECTORIO?

En la mayoría de las redes, usted optimiza la función de diferentes servicios almacenándolos en diferentes computadoras. Este procedimiento tiene sentido. Poner todos sus servicios en una computadora es muy similar a poner todos los huevos en una canasta: si se cae la canasta, se rompen todos los huevos. Además, puede alcanzar un óptimo desempeño, más confiabilidad y mayor seguridad si segrega los servicios de red de diferentes maneras. La mayoría de las redes tienen muy pocos servicios que necesitan ofrecerse y a menudo corren en servidores diferentes. Aun una red relativamente simple ofrece los servicios siguientes:

- Almacenamiento y compartición de archivos
- Compartición de archivos
- Servicios de correo electrónico
- Anfitrión de web, para Internet y para intranet
- Servidor de base de datos
- Servicios de aplicación específica
- Conectividad a Internet
- Servicios de marcación entrante y saliente
- Servicios de fax
- Servicio de Sistema de Nombre de Dominio (DNS), Servicios de Nombres de Windows de Internet (WNS)
- Servicios centralizados de detección de virus

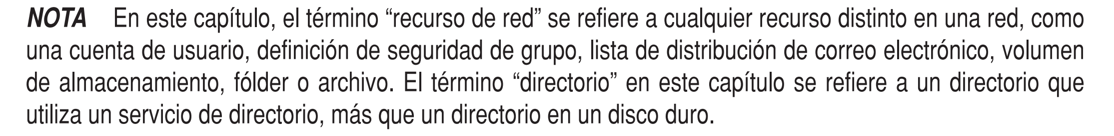
Ésta es solo una pequeña lista. Las organizaciones más grandes tienen servidores múltiples que comparten estas funciones —con diferentes servicios disponibles a través de dife-

rentes medios en cada edificio o ubicación— y deben tener servicios adicionales a los que se analizan aquí.

Toda esta complejidad puede generar una red caótica y muy difícil de manejar. Si cada servidor individual requiere una administración independiente (por ejemplo, con listas separadas de usuarios, grupos, impresoras, configuraciones de red, etc.), entonces usted puede fácilmente ver cómo el trabajo se puede convertir en algo virtualmente imposible.

Los *servicios de directorio* se inventaron para organizar las redes. Básicamente, trabajan como la sección amarilla. En lugar de utilizar un nombre para tratar de encontrar una dirección y un número telefónico, usted consulta el servicio de directorio para buscar un nombre de servicio (como el nombre del fólder de la red, o una impresora), y el servicio de directorio le dice dónde puede localizarlo. También puede consultar servicios de directorio por propiedad. Por ejemplo, si consulta el servicio de directorio de todos los artículos que sean "impresoras", puede proporcionar como respuesta una lista completa, sin importar dónde estén localizadas las impresoras dentro de la organización. Aún mejor, los servicios de directorio le permiten navegar por todos los recursos de una red, de manera fácil, en una lista unificada organizada en una estructura de árbol.

Una ventaja importante de los servicios de directorio es que eliminan la necesidad de manejar duplicados de la información en la red, ya que el directorio es automáticamente compartido entre todos los servidores. Por ejemplo, usted no debe tener listas de usuarios separados en cada servidor. En lugar de eso, administra un solo conjunto de cuentas de usuario que existen en el servicio de directorio y después les asigna varios derechos a recursos en particular en cualquiera de los servidores. Otros recursos trabajan de la misma forma y se administran de manera central en el servicio de directorio. Esto no solo significa que usted tiene una colección de objetos por administrar, sino también que los usuarios cuentan con una manera más sencilla de experimentar en la red. Desde la perspectiva del usuario, solo existe una cuenta de red con una contraseña y no se tiene que preocupar acerca de dónde se encuentran los recursos o de rastrear las diferentes contraseñas de los diferentes servicios de red y servidores.



NOTA En este capítulo, el término "recurso de red" se refiere a cualquier recurso distinto en una red, como una cuenta de usuario, definición de seguridad de grupo, lista de distribución de correo electrónico, volumen de almacenamiento, fólder o archivo. El término "directorio" en este capítulo se refiere a un directorio que utiliza un servicio de directorio, más que un directorio en un disco duro.

Para proporcionar redundancia, por lo general, los servicios de directorio de una organización corren en múltiples servidores y cada uno cuenta con una copia completa de la base de datos del directorio. Las bases de datos separadas se mantienen en sincronía mediante un proceso llamado *replicación*, en el que los cambios en cualquiera de las bases de datos de directorio individuales se actualizan, de manera transparente, con todas las demás bases de datos del servicio de directorio. Debido a que estos servicios se convierten en parte central del funcionamiento de una red, este método permite que toda la red continúe en operación en caso de que cualquier servidor que cuente con servicios de directorio falle. En realidad, los servidores que no almacenan una copia del directorio aún pueden utilizarlos comunicándose con los servidores de directorio. Por ejemplo, si un usuario trata de abrir un archivo almacenado en un servidor que no almacena el servicio de directorio, el servidor automáticamente consultará el servicio de directorio en otro servidor para autentificar la solicitud de acceso del usuario. Para el usuario, este proceso sucede tras bambalinas.

Usted debe conocer acerca de los cinco servicios de directorios importantes:

- *eDirectory de Novell* (anteriormente llamado Servicio de Directorio de Novell o DNS) es el servicio de directorio de red que ha sido popular durante un mayor periodo. eDirectory corre en NetWare 4.x y servidores más grandes y se encuentra disponible en otros sistemas operativos de servidor (como Solaris, Linux y Windows NT), lo cual permite utilizarlo como un solo servicio de directorio para la administración de una red de múltiples fabricantes.
- *Los dominios de Windows NT* no son, en realidad, servicios de directorio completos, pero ofrecen algunas de las características y ventajas de los servicios de directorio.
- *Directorio Activo de Microsoft* hizo su debut con la línea de productos de servidores de Windows 2000. Éste es un verdadero servicio de directorio, pues ofrece todas las características de éste, a una red predominantemente construida con Windows 2000 Server y Windows Server 2003.
- *Protocolo X.500 de Acceso a Directorio (DAP)* es un servicio de directorio estándar internacional que tiene muchas capacidades. Sin embargo, X.500 proporciona tantos atributos que su información de relleno hace prohibitivo su uso y administración. En consecuencia, el X.500 es una posición interesante: es un estándar importante pero, paradójicamente, no se utiliza en realidad.
- El *Protocolo de Acceso a Directorios Livianos (LDAP)* fue desarrollado por un consorcio de fabricantes como un subconjunto de X.500 para ofrecer una alternativa con menor complejidad que éste. LDAP se utiliza ampliamente en directorios de correo electrónico y es apropiado para otras tareas de servicio de directorio. Las versiones más recientes de eDirectory —y también Active Directory— son compatibles con LDAP.

Bosques, árboles, raíces y hojas

Una cosa en común de todos los servicios de directorio en una organización basada en árboles (con el árbol generalmente dibujado al revés, esto es, con la raíz en la parte superior), de alguna forma similar a la organización de directorios en el disco duro. En la parte más alta del árbol están las entradas de las raíces, las cuales contienen otras entradas que pueden ser contenedores u hojas. Un *objeto contenedor* es uno que contiene otros objetos, los cuales también pueden incluir más contenedores y hojas. Un *objeto hoja* representa un recurso real de la red, como una estación de trabajo, una impresora, un directorio compartido, un archivo o una cuenta de usuario. Los objetos representados por las hojas no pueden contener otros objetos. La figura 9-1 muestra un árbol de directorio típico.

Todos los objetos en un árbol de directorios tienen *atributos* (a veces llamados *propiedades*), que varían en función del tipo de objeto al que el atributo está conectado.

Por ejemplo, un *objeto hoja de una impresora* puede contener atributos que describan la impresora, quién puede administrarla, cuál es su nombre en la red, etc. Un *objeto hoja de la cuenta de usuario* puede contener atributos que incluyan el nombre completo de la cuenta de usuario, su contraseña y los recursos a los que puede acceder. Los detalles de qué atributos están conectados a qué objetos hoja o contenedor varían entre todos los servicios de directorio, aunque, generalmente, éstos utilizan atributos similares.

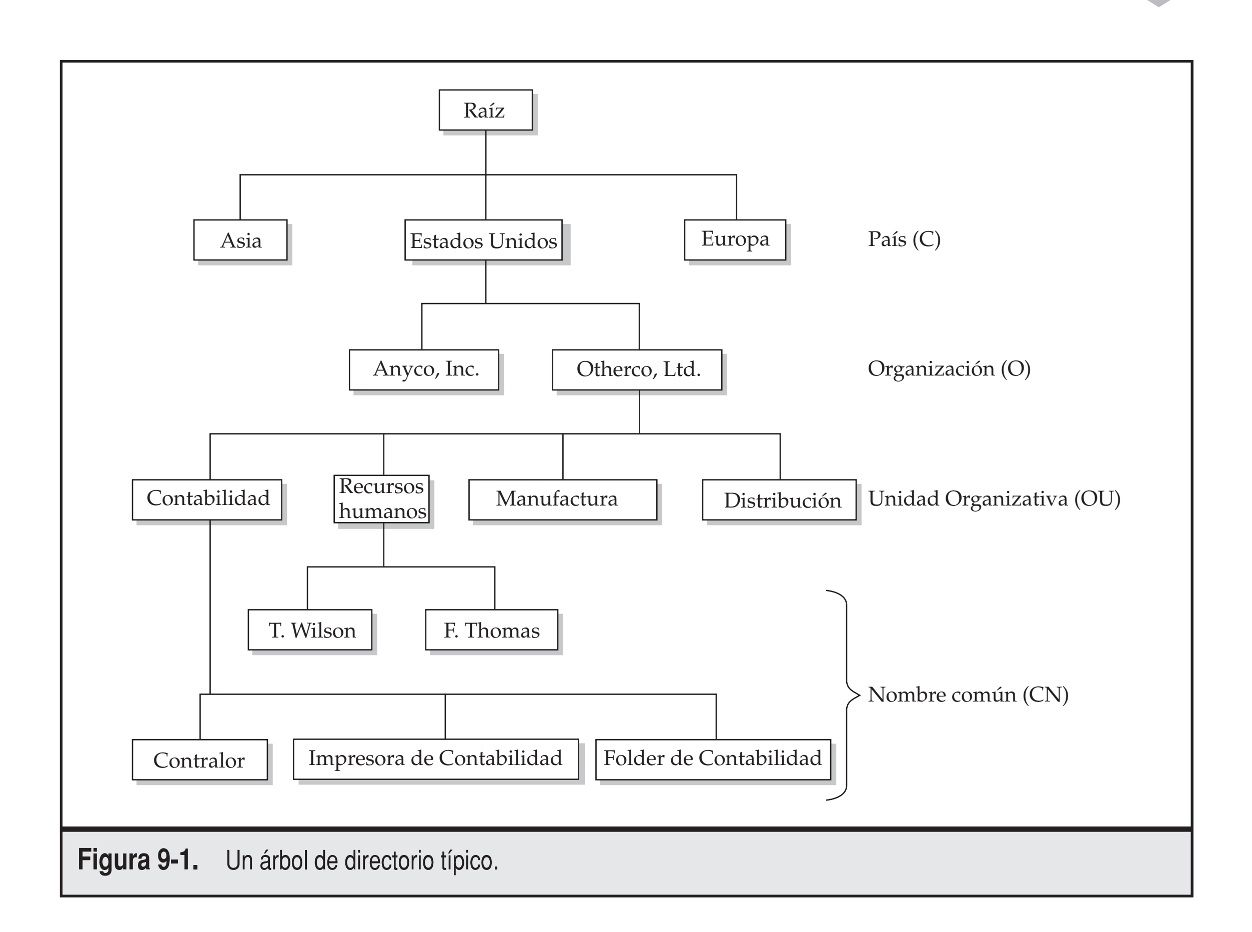


Figura 9-1. Un árbol de directorio típico.

Departamento del departamento de redundancia

Mantener en operación a los servicios de directorio es esencial para cualquier red que dependa de ellos. Debido a que contienen todos los detalles acerca de las cuentas, recursos y seguridad, su ausencia significa que la red no va a funcionar plenamente. Debido a que los servicios de directorio se convierten en algo muy importante para una red, usted debe protegerlos con algún grado de redundancia. Mantener un duplicado de copias del directorio en servidores múltiples proporciona la redundancia necesaria. Lo anterior se lleva a cabo mediante uno o más métodos: principal/respaldo (también llamado maestro/esclavo) y multimaestro. En el *modelo principal/respaldo*, una sola base de datos principal contiene el directorio principal (o "real") en un servidor, mientras que otros servidores conservan una o más copias de respaldo. Si la copia principal deja de funcionar por alguna razón, los respaldos pueden continuar ofreciendo los servicios de directorio a la red sin que el usuario siquiera sepa que la copia principal no está disponible. Los dominios de Windows NT utilizan un método principal/respaldo. En el *modelo multimaestro*, existen múltiples servidores de directorio, pero éstos se encuentran en el mismo nivel entre sí. Si uno falla, los demás continúan trabajando de manera normal. La ventaja del modelo multimaes-

tro es que cada servidor de directorio puede participar totalmente en la realización del trabajo del servicio de directorio. El Directorio activo (en Windows 2000 Server y Windows Server 2003) utiliza el método multimaestro.

Los servicios de directorio, ya sea que utilicen el método principal/respaldo o el multimaestro, deben conservarse en sincronía con los cambios de la red. Esta sincronización se proporciona por medio de un proceso llamado replicación, que automáticamente duplica cualquier cambio en el directorio en un servidor en todos los demás servidores de directorio.

Sin embargo, existe un problema potencial en cualquier proceso de replicación: si se realizan dos cambios al mismo objeto hoja en dos servidores de directorio diferentes y los cambios son diferentes, ¿qué hará el sistema cuando los cambios "choquen" durante el proceso de replicación? Los diferentes servicios de directorio manejan este problema de formas ligeramente diferentes. En el caso de eDirectory, las marcas de tiempo de los cambios definen cuál de las dos modificaciones en conflicto ganará. (Debido a esto, los servidores que corren eDirectory deben mantener su tiempo sincronizado; esta sincronización también es manejada durante la replicación). El Directorio Activo de Microsoft no utiliza marcas de tiempo; en lugar de ello, utiliza una secuencia de números en un esquema muy inteligente que evita los problemas potenciales asociados con el método de las marcas de tiempo. (A pesar de que los servidores eDirectory sincronizan su tiempo, su temporización puede aún estar fuera de sincronía entre sincronizaciones).

Algunos servicios de directorio también admiten una facilidad llamada *particionamiento*, en la cual diferentes servidores de directorio conservan las partes del árbol de todo el directorio. En este caso, un servidor controlador de directorio generalmente administra todo el árbol (se llama *catálogo global* en Active Directory), y después otros servidores de directorio pueden administrar pequeñas porciones de todo el árbol. El particionamiento es importante en las redes con múltiples LAN conectadas por una WAN. En dichos casos, usted quisiera almacenar localmente una partición que se relacionara a una LAN particular pero, a la vez, permitir el acceso al árbol completo para acceder a recursos a través de la WAN. Cada LAN almacena su propia partición, pero aun puede acceder al árbol total cuando sea necesario. Usted arregla la partición (y fija los tiempos de replicación programados) para hacer uso óptimo del desempeño de la WAN, el cual generalmente es menor que el de una LAN.

SERVICIOS ESPECÍFICOS DE DIRECTORIO

Existen muy pocos servicios de directorio. La selección de uno de ellos, generalmente, va de la mano con la selección de un sistema operativo de red principal (NOS), aunque éste no es siempre el caso. Tanto el eDirectory como el Active Directory pueden manejar servidores que no sean Novell ni Microsoft, respectivamente. En consecuencia, aun una red que actualmente utilice en su mayoría servidores Windows NT, puede depender en eDirectory para los servicios de directorio mediante el uso de eDirectory de Novell para el producto Windows NT. La utilización de un solo servicio de directorio con sistemas operativos de red diferentes a menudo sucede debido a que una organización al principio favorece a un sistema operativo de red en particular y, después, se ve forzada a soportar NOS adicionales, pero la organización aún desea conservar un único servicio de directorio para administrar ambos sistemas operativos de red.

En secciones anteriores dentro de este capítulo se proporcionó una lista de los principales servicios de directorio. Aquí se mencionan de nuevo:

- eDirectory de Novell
- Dominios de Windows NT de Microsoft
- Active Directory de Microsoft
- Protocolo de Acceso a Directorio (DAP) X.500
- Protocolo Ligero de Acceso a Directorio (LDAP)

Éstos son los servicios de directorio predominantes que usted encontrará, aunque debe estar consciente de que existen otros. Por ejemplo, un gran número de compañías ofrecen software diferente que proporciona servicios de directorio que cumplen con el protocolo LDAP en plataformas diferentes. Asimismo, algunos servicios de directorio anteriores como Banyan Streettalk o SecureWay Directory, de IBM, pueden encontrarse en redes que no hayan sido actualizadas.

eDirectory

eDirectory de Novell (originalmente llamado Novell Directory Services, o NDS) ha estado disponible desde 1993, cuando fue presentado como parte de NetWare 4.x. Con un gran número de organizaciones que tienen decenas o cientos de servidores NetWare, este producto fue un verdadero "boom" y se implementó muy rápido, particularmente en organizaciones grandes que necesitaban desesperadamente sus virtudes. eDirectory es un servicio confiable y robusto que ha seguido evolucionando desde su introducción. En la actualidad está disponible la versión 8.7, que incorpora las últimas capacidades del servicio de directorio.

eDirectory utiliza un método maestro/esclavo en los servidores de directorio y también permite la partición del árbol. Además de correr sobre los sistemas operativos de red Novell, eDirectory está también disponible en sistemas Windows, Solaris, HP/UX, AIX y Linux. La compatibilidad del producto con dicha variedad de sistemas hace de eDirectory una buena opción para la administración de todas estas plataformas bajo una sola estructura de directorios.

Usted administra el árbol eDirectory desde una computadora cliente que esté conectada a la red con privilegios administrativos. Usted puede utilizar herramientas gráficas diseñadas para administrar el árbol, como Novell Manager, u otras que imiten la apariencia del sistema operativo sobre el que trabajan y que se encuentren disponibles por medio de Novell.

El árbol eDirectory contiene un gran número de tipos de objetos diferentes. Los tipos de servicio de directorio estándar incluyen países, organizaciones y unidades organizacionales. El sistema también cuenta con objetos que representan grupos de seguridad de NetWare, servidores y volúmenes de servidores NetWare. eDirectory puede administrar más de un billón de objetos en un árbol.

Dominios de Windows NT

Windows NT 4 introdujo al mercado una característica de servicio de directorio organizada por medio del uso de dominios. El modelo de Windows NT divide una organización en fragmentos llamados dominios, cada uno de los cuales son parte de ella. Por lo general, los dominios están organizados geográficamente, lo cual ayuda a minimizar los requerimientos de comunicación de dominio a dominio a través de los enlaces WAN, aunque usted puede sentirse con toda la libertad de organizar los dominios como lo desee. Cada dominio está controlado por un *Controlador de*

dominio principal (PDC), el cual puede tener uno o más *Controladores de Dominio de Respaldo (BDCs*) para el caso de que el PDC falle.

Todos los cambios que se introducen a un dominio se realizan dentro del PDC, el cual replica los cambios en cualquiera de los BDC, que son de solo lectura, excepto para actualizaciones válidas recibidas del PDC. En el caso de una falla en un PDC, los BDC automáticamente siguen autentificando a los usuarios. Para realizar cambios administrativos a un dominio que sufre de una falla en el PDC, cualquiera de los BDC puede ser *promovido* a PDC. Una vez que el PDC está listo para volver a estar en línea, el BDC promovido puede *regresar* a su estatus anterior.

Los dominios en Windows NT pueden estar organizados en uno de cuatro modelos de dominio. Usted selecciona uno apropiado en función de la distribución física de la red, el número de usuarios a servir y otros factores. (Si usted está planeando un modelo de dominio, debe revisar los planos en el sitio web de Microsoft acerca de la planeación de dominios grandes, ya que el proceso puede ser muy complejo).

Los cuatro modelos de dominio son:

- **Dominio único** En este modelo, solo un dominio contiene los recursos de la red.
- **Dominio maestro** El modelo maestro generalmente coloca a los usuarios en el dominio más alto y después ubica los recursos de la red, como los fólders o impresoras compartidas en los dominios de más bajo nivel (llamados dominios de recursos). En este modelo, los dominios de recursos confían en el dominio maestro.
- **Dominio maestro múltiple** Éste es una ligera variación del modelo del dominio maestro, en el cual los usuarios pueden existir en múltiples dominios maestros, los que dependen el uno del otro y en el que los recursos están ubicados en los dominios de recursos, todos los cuales dependen de todos los dominios maestros.
- **Confianza total** Esta variación del modelo de dominio único distribuye a los usuarios y los recursos a través de todos los dominios, los cuales dependen uno del otro.

Las relaciones de confianza explícitas deben conservarse entre los dominios que utilizan los modelos maestros o de dominio maestro múltiple y administrarse en cada dominio de manera separada. La conservación de estas relaciones es una de las dificultades más grandes del método de la estructura de dominios de Windows NT, por lo menos en grandes organizaciones; si usted tiene 100 dominios, debe administrar las 99 relaciones de confianza posibles para cada dominio dentro de cada uno de éstos, lo que significa un total de 9 900 relaciones de confianza. Para un número más pequeño de dominios (por ejemplo, menos de 10 dominios), la administración de las relaciones de confianza no representan un gran problema, aunque aún pueden causar dificultades.

Directorio activo

Los dominios de Windows NT trabajan relativamente bien en redes pequeñas, pero pueden ser difíciles de administrar en redes grandes. Además, el sistema no es tan detallado como eDirectory. Microsoft reconoció este problema y desarrolló un servicio de directorio llamado Directorio Activo, que es un servicio detallado que corre sobre Windows 2000 Server y Windows Server 2003. El Directorio Activo es totalmente compatible con LDAP (versiones 2 y 3) y también con el DNS utilizado en Internet.

El Directorio Activo utiliza un método de igual a igual para los controladores de dominio; todos éstos participan totalmente en todo momento. Como se mencionó anteriormente, este arreglo se llama *multimaestro* debido a que existen muchos controladores de dominio "maestro", pero no controladores "esclavo".

El Directorio Activo está construido sobre una estructura que permite "árbol de árboles", lo cual se llama un bosque. Cada árbol tiene su propio dominio y sus controladores de dominio. Dentro de un dominio se permite que unidades organizacionales separadas hagan la administración más fácil y más lógica. Los árboles se encuentran, entonces, agregados mediante una estructura de árbol más grande. De acuerdo con Microsoft, Active Directory puede manejar millones de objetos por medio de este método.

El Directorio Activo no requiere la administración de relaciones de confianza, excepto cuando está conectado a servidores Windows NT 4.*x* que no utilicen Active Directory. De otra forma, todos los dominios dentro de un árbol tienen relaciones de confianza automática.

X.500

El estándar X.500 fue desarrollado conjuntamente por la Unión Internacional de Comunicaciones (ITU) y la Organización Internacional de Estándares (ISO). El estándar define un servicio de directorio que puede utilizarse para todo Internet. Debido a su amplia aplicación, la especificación X.500 es demasiado compleja para implantarse en la mayoría de las organizaciones. Asimismo, debido a su diseño, está orientada hacia la publicación de parámetros específicos de directorio organizacional a través de Internet, lo cual es algo que la mayoría de las compañías no quieren hacer. De la misma forma, el estándar X.500 es extremadamente importante y la mayoría de los servicios de directorio imitan o incorporan partes de él de alguna forma.

El árbol de directorios de X.500 comienza con una raíz, de la misma forma que los árboles de directorio, la cual después se divide en campos, esto es, país (C), organización (O), unidad organizativa (OU) y nombre común (CN). Para especificar totalmente una dirección X.500, usted proporciona cinco campos, de la manera siguiente:

```
CN=user name, OU=department, OU=division, O=organization, C=country
```

Por ejemplo, usted puede configurar los campos como sigue:

```
CN=Bruce Hallberg, OU=Networking Books, OU=Computer Books, O=McGraw-Hill,
C=USA
```

LDAP

Para solucionar la complejidad de los problemas asociados con todo el DAP de X.500, un consorcio de compañías sacó un subconjunto de X.500 llamado Protocolo Ligero de Acceso a Directorios (LDAP). Los seguidores de LDAP dicen que éste proporciona 90% de las capacidades de X.500, pero solo a 10% del costo de procesamiento. LDAP corre sobre TCP/IP y utiliza un modelo cliente/servidor. Su organización es muy parecida a la de X.500, pero con menos campos y menos funciones.

HLDAP está definido básicamente, en el RFC 1777 (versión 2) y el RFC 2251 (versión 3). Algunos otros RFC también describen aspectos de LDAP; sin embargo, 1777 y 2251 son los dos documentos principales. El estándar LDAP describe no solo la distribución y los campos

dentro del directorio LDAP, sino también los métodos por utilizarse cuando una persona firma en el servidor que utiliza LDAP, consulta o actualiza la información en el directorio de LDAP en un servidor LDAP. (Debido a que los servicios de directorio deben cumplir con muchas autentificaciones simultáneas, las consultas y pueden aceptar actualizaciones simultáneas, es importante que estos métodos sean definidos claramente a fin de evitar colisiones y el mal uso del directorio por parte de las aplicaciones del cliente y herramientas administrativas).



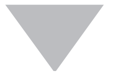
NOTA Muchos de los estándares de Internet están controlados por documentos llamados Solicitudes de comentarios (RFC), documentos que describen un estándar propuesto y se someten al grupo de Fuerza de Tarea de Ingeniería de Internet. Usted puede leer más acerca de este grupo, así como examinar cualquiera de los RFC de conectividad de redes que se mencionen en este libro (o en cualquier otra parte) en el sitio en Internet **http://www.ietf.org**.

Modelos de LDAP

Los cuatro modelos básicos siguientes describen el protocolo LDAP:

- El *Modelo de información* define la estructura de datos almacenados en el directorio.
- El *Modelo de asignación de nombres* define cómo organizar y referirse a los datos.
- El *Modelo funcional* define cómo trabajar con los datos.
- El *Modelo de seguridad* define cómo conservar seguros los datos en el directorio.

El Modelo de información describe una gran cantidad de aspectos del directorio. Primero se encuentra el *esquema*, que es un machote del directorio y sus parámetros. Después se encuentran las clases permitidas de los parámetros del directorio. Las clases son categorías a las cuales todos los parámetros se encuentran conectados. Después, el Modelo de información define los *atributos*, que son la parte de los datos que describen las clases. Un ejemplo de un atributo es CN o OU, que son atributos utilizados para todos los parámetros en el directorio. El siguiente aspecto descrito por el Modelo de información es la *sintaxis* de los atributos. La sintaxis especifica exactamente cómo se denominan los atributos, cómo se almacenan y qué tipo de datos se les permite contener (como nombres, series de texto, fechas y horas, etc.). Por último, se definen los *parámetros*. Un parámetro es una porción de datos distinta, como un objeto, que puede ser tanto un contenedor como una hoja.



NOTA Microsoft utiliza la nomenclatura para describir LDAP que difiere de los términos definidos en los RFC. Dentro de los principales, Microsoft llama objeto a un parámetro y propiedad a un atributo. Estos nombres se refieren a las mismas cosas, y usted debe estar consiente de ello cuando lea los RFC u otros documentos acerca de LDAP y cuando compare esta información con la que se presenta en los documentos de Microsoft.

El Modelo de asignación de nombres define los nombres que sirven como claves principales para los parámetros en el directorio. De esta forma, define *nombres distinguidos (DN)*, que son nombres completos de parámetros, así como *nombres distinguidos relativos (RDN)*, que son componentes de Nombres distinguidos. Lo que sigue es un ejemplo de un DN de LDAP:

```
CN=Bruce Hallberg, OU=Networking Books, OU=Computer Books, O=McGraw-Hill,
C=USA
```

Cada componente del DN, como los parámetros CD, OU u O, es un RDN.

El Modelo funcional de LDAP define cómo lleva a cabo tres tipos de operaciones: autentificación, interrogación y actualizaciones. La autentificación es el proceso por el cual los usuarios demuestran su identidad al directorio, interrogación es aquel mediante el cual se consulta la información que contiene el directorio, mientras que actualizaciones son operaciones que sugieren cambios en el directorio.

Por último, el Modelo de seguridad controla cómo un directorio se utiliza en forma segura. En la mayoría de las implantaciones de LDAP, se utiliza un protocolo de seguridad llamado Capa de seguridad y autentificación simple (SASL). El RFC 2222 describe SASL.

Organización del LDAP

Un árbol LDAP comienza en la raíz, la cual contiene parámetros. Cada parámetro puede tener uno o más *atributos*. Cada atributo tiene tanto un *tipo* como *valores* asociados con él. Un ejemplo es el CN, que contiene al menos dos atributos: FirstName y Surname (nombre propio y apellido). Todos los atributos en LDAP utilizan el tipo de datos de texto encadenado. Los parámetros están organizados en un árbol y administrados geográficamente y, después, dentro de cada organización.

Una característica muy atractiva de LDAP es que una organización puede construir una estructura global de directorios utilizando una característica llamada *referencia*, donde las consultas al directorio LDAP que son administradas por un servidor LDAP diferente se enrutan, de manera transparente, a ese servidor. Debido a que cada servidor LDAP conoce su servidor LDAP pareja y sus servidores hijos, cualquier usuario en cualquier punto de la red puede acceder a todo el árbol. En realidad, el usuario ni siquiera sabrá que está accediendo a diferentes servidores ubicados en lugares diferentes.

RESUMEN DEL CAPÍTULO

En este capítulo aprendió acerca de la importancia de los servicios de directorio y los factores que determinan dicha importancia. Asimismo, aprendió cómo funcionan los servicios de directorio, qué tareas llevan a cabo y las características comunes que se encuentran en casi todos los servicios de directorio. Por último, se analizaron los servicios de directorio más importantes, entre ellos el eDirectory de Novell, el servicio de dominio Microsoft y el servicio de Active Directory.

El capítulo siguiente es una continuación de los análisis acerca de las tecnologías y servicios esenciales de las redes, y le enseña acerca de los servicios de acceso remoto, con los cuales los usuarios que se encuentran muy esparcidos en la red pueden acceder a las LAN desde cualquier lugar del mundo. La implantación de un buen sistema de acceso remoto con el que todos estén contentos es una de las tareas más difíciles de llevar a cabo —especialmente en organizaciones de gran tamaño que tengan necesidades muy diversas—por lo que se analiza una gran variedad de técnicas.



CAPÍTULO 10

Conexiones a larga distancia: acceso remoto a redes

En los capítulos anteriores usted aprendió acerca de los sistemas de conectividad de redes a través de una LAN y una WAN, y sobre las tecnologías que operan en ambos tipos de redes. Ahora, también necesita saber acerca de otro tipo de conexión que es muy importante: el acceso remoto a redes. En las culturas corporativas actuales de "viaje feliz" y en las compañías que necesitan de soporte para que su personal trabaje desde casa y en pequeñas oficinas a distancia, el acceso remoto se ha hecho más importante que nunca. Desafortunadamente, también es una de las partes más difíciles de realizar en una red, como podrá observar en este capítulo.

Uno de los grandes problemas del acceso remoto es que puede parecer como si los usuarios remotos tuvieran diferentes necesidades, todas las soluciones disponibles sirvieran a necesidades distintas y ninguna de ellas atendiera todas las necesidades. Analizar las necesidades de su compañía y encontrar soluciones sólidas que cumplan con ellas es, generalmente, difícil y requiere de mucho tiempo y esfuerzo. La sección siguiente describe una forma en la que puede clasificar las necesidades del acceso remoto, que es el primer paso en la búsqueda de una solución (o soluciones) para el acceso remoto de su red.

CLASIFICAR A LOS USUARIOS REMOTOS

Los usuarios que requieren acceso remoto caen en una de muchas categorías. A menudo, cada categoría de usuario remoto tiene necesidades diferentes y, con frecuencia, las distintas tecnologías y soluciones de acceso remoto son necesarias para cumplir estas necesidades por completo. Lo más importante que debe recordar es que necesita conocer a qué categorías de usuarios remotos tiene que proporcionar soporte; cada compañía tiene una mezcla diferente, cuyas necesidades cambian de empresa a empresa. Además, aun cuando las necesidades fueran idénticas, las soluciones que emplee pueden cambiar con base en otro criterio. Por ejemplo, usted puede manejar el acceso a un sistema de contabilidad desde un punto remoto de forma diferente, en función de eso es un cliente/servidor o una aplicación monolítica.

Sugiero que clasifique a sus usuarios de acceso remoto en una de las cuatro categorías siguientes:

- Viajero muy frecuente
- Viajero no tan frecuente
- Usuario de oficina remota
- Grupo de oficina remota

Usted necesita diferentes estrategias para soportar a estos diferentes usuarios. Si trabaja en una compañía pequeña, es muy probable que no requiera todas estas categorías en este momento.

El tipo de usuario de acceso remoto más común se llama *viajero muy frecuente*, que es alguien que normalmente tiene como base una oficina principal donde, en general, tiene acceso a LAN, pero que ocasionalmente o muy a menudo viaja de negocios, y además tiene que viajar virtualmente a cualquier lugar del mundo, por lo que debe lidiar con diferentes sistemas telefónicos, empresas de larga distancia y otros problemas de tipo geográfico (vea la figura 10-1). Muy a menudo, este tipo de usuario necesita acceder al servicio de correo electrónico; sin embargo, en ocasiones, también necesita archivos almacenados o enviados por este medio. Este usuario pue-

¡DEFÍNALO! Aplicaciones cliente/servidor

Las aplicaciones cliente/servidor consisten en procesos (programas) que corren tanto del lado del servidor como del cliente y que trabajan al unísono. Por ejemplo, un servidor de base de datos atiende consultas del cliente y después transmite al cliente sólo los resultados de dicha consulta. El trabajo del cliente es solamente desplegar los resultados y quizá formatearlos para su impresión. Por otro lado, una aplicación monolítica lleva a cabo todo su trabajo en una computadora, que por lo general es la computadora del cliente. El servidor de una aplicación monolítica da servicio solamente a los archivos necesarios para que corra la aplicación y a los archivos de datos que la aplicación manipula. En general, las aplicaciones cliente/servidor requieren menos ancho de banda para trabajar a velocidades aceptables que las aplicaciones monolíticas. Una conexión lenta de red podría ser adecuada para una aplicación cliente/servidor, como en un sistema de contabilidad, mientras que el mismo módem sería totalmente inapropiado para esa misma aplicación, pero diseñada para ser monolítica.

de o no tener una computadora (laptop) portátil asignada. El usuario normalmente utiliza una computadora de escritorio conectada a la LAN, pero cuenta con una laptop para viajar; o puede utilizar solo una tanto en la LAN como cuando se encuentra de viaje, puede seleccionar una computadora portátil de un grupo compartido en su compañía cuando necesite viajar, e incluso, puede rentar una computadora laptop en caso de un viaje ocasional. Estos diferentes escenarios complican aún más el proporcionar servicios al viajero.

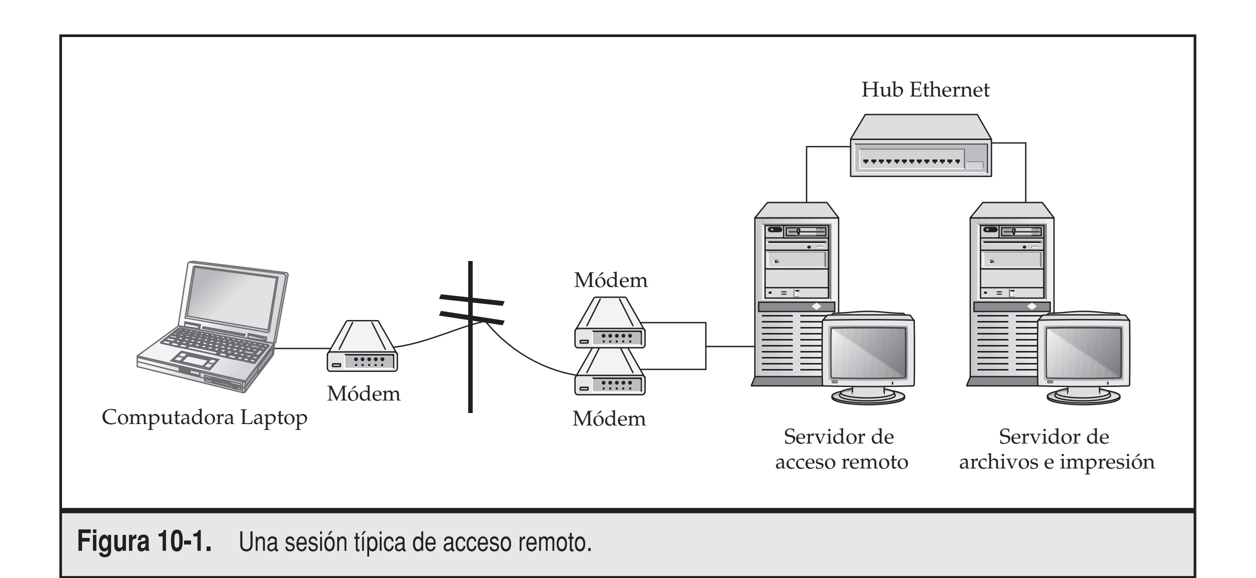


Figura 10-1. Una sesión típica de acceso remoto.

Otra tipo común de usuario de acceso remoto se llama el *viajero no tan frecuente*, quien viaja relativamente a pocos lugares, como de la oficina matriz a las plantas de manufactura o centros de distribución. El aspecto atractivo de este usuario es que es posible predecir los sitios en donde puede necesitar acceso a datos y, por tanto, se puede poner a su disposición el soporte local en el lugar, con el fin de ayudarlo. Por ejemplo, puede implantar una forma para que el usuario se firme en la LAN de un centro de distribución y así, tenga acceso a su correo electrónico y a archivos de la oficina matriz a través de un enlace WAN, como se muestra en la figura 10-2. Este tipo de usuario necesita correo electrónico, acceso a archivos y, a menudo, acceso a una aplicación centralizada como un sistema de contabilidad.

El tercer tipo de usuario de acceso remoto es el *usuario de oficina remota*, quien se encuentra en un solo lugar y necesita tener acceso a una LAN corporativa para entrar a su correo electrónico y, posiblemente, para utilizar aplicaciones (ver figura 10-3). Esta persona generalmente no necesita tener acceso a archivos, excepto para enviarlos a través del correo electrónico, ya que tiene un almacenamiento local de archivos. Este usuario se encuentra en un solo punto, por lo que usted puede instalar cierto tipo de enlace de alta velocidad que no es factible en el caso de los usuarios viajeros. Una persona que vaya y venga de su casa al trabajo caería en esta categoría de usuario de oficina remota.

El cuarto tipo de usuario de acceso remoto, el *grupo de oficina remota*, es un híbrido. A veces un pequeño grupo (de dos a cinco personas) ubicado en un lugar remoto necesita ciertos servicios de una LAN corporativa, por lo que no es costeable que cuente con estos servicios localmente, aun cuando tengan una pequeña LAN local que les permita compartir impresoras y archivos, como se puede observar en la figura 10-4. Este tipo de usuarios de acceso remoto necesita una

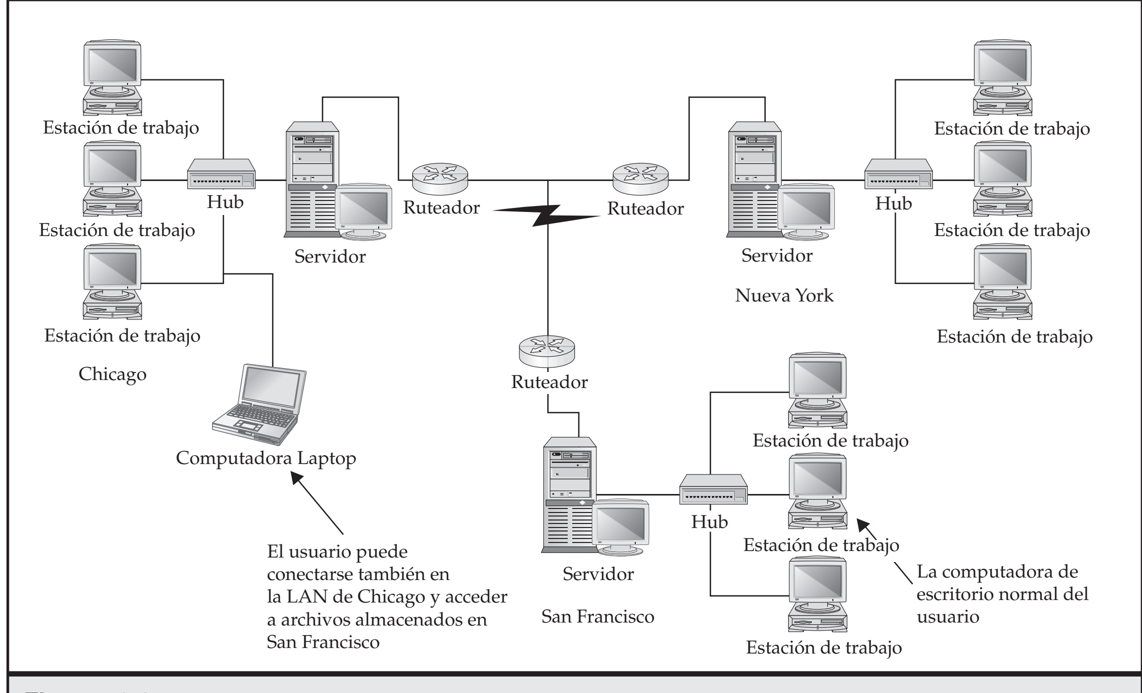


Figura 10-2. Una LAN utilizada por un "viajero poco frecuente".

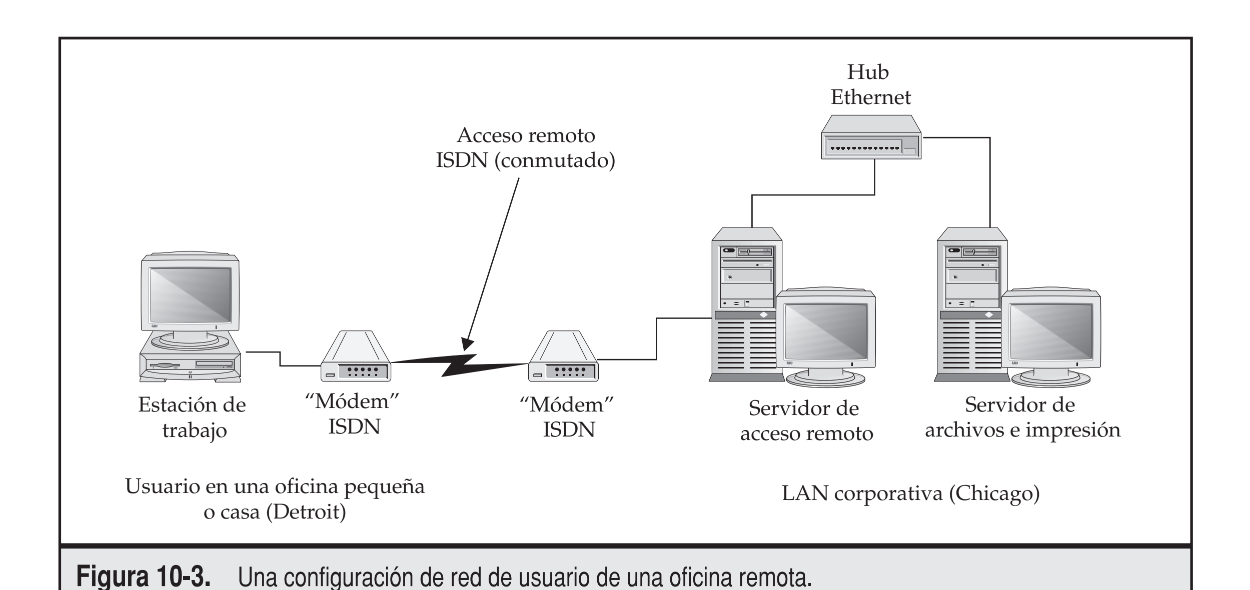


Figura 10-3. Una configuración de red de usuario de una oficina remota.

Estación de trabajo
Estación de trabajo
Estación de trabajo
Oficina remota
Hub
Servidor de
archivos e impresión
Ruteador
Ruteador
LAN corporativa principal
Servidor de
archivos e impresión
Hub
Estación de trabajo
Estación de trabajo
Estación de trabajo

Los usuarios de oficinas remotas utilizan el servidor local de archivos e impresión, sin embargo, pueden acceder al servidor de base de datos corporativo a través de una conexión de área amplia.

El enlace de la oficina remota a la LAN corporativa puede ser dedicado o conmutado. Por ejemplo, un enlace ISDN por demanda o un enlace xDSL pueden ser ambos buenas soluciones para la conexión WAN.

Servidor de base de datos del sistema de ingreso de órdenes/rastreo de ventas.

Figura 10-4. Soporte de una pequeña oficina remota que requiere acceder a una LAN.

combinación de servicios: en parte son como cualquier usuario de una LAN remota y también son como un usuario de oficina remota. Estos usuarios, en general, requieren una mezcla de ambos tipos de soluciones para proporcionarles el soporte adecuado.

DETERMINAR LAS NECESIDADES DE ACCESO REMOTO

Antes de implantar cualquier sistema de acceso remoto, usted necesita definir de manera clara cuáles son las necesidades de los diferentes tipos de usuarios remotos de la empresa. Algunos ejemplos de necesidades que debe satisfacer son:

- Acceso remoto fácil al correo electrónico y a archivos almacenados en éste.
- Acceso remoto a archivos privados o compartidos almacenados en la LAN.
- Acceso remoto a una aplicación centralizada, como un sistema de contabilidad o un sistema de órdenes de venta.
- Acceso remoto a programas de groupware o aplicaciones personalizadas.
- Acceso a Internet.
- Acceso a Internet/extranet, que incluye cualquier aplicación basada en la web que esté almacenada en estos sistemas.
- Acceso remoto a cualquiera de las características anteriores desde una ubicación fija, como una oficina de ventas remota.
- Acceso remoto a cualquiera de las características anteriores desde cualquier lugar del mundo.

Para comprender sus necesidades específicas de soporte de acceso remoto, es importante que entreviste a todos los usuarios potenciales (o al menos a un subconjunto representativo) y busque la manera de clasificarlos como se describió antes. Es probable que deba soportar el acceso remoto por medio de más de un mecanismo. La forma como clasifique a los usuarios y sus necesidades le sugerirá qué mecanismo tiene más sentido.

Cuando entreviste a los usuarios, asegúrese de que haya considerado todas las necesidades posibles. Por ejemplo, al preguntarles si necesitan acceso remoto a los archivos almacenados en sus directorios LAN y ellos contestan: “en realidad no”, esa no es una respuesta adecuada. Es necesario que usted los presione formulándoles preguntas como: “¿Alguna vez necesitará acceso remoto a los archivos? ¿Qué sucede si solo tiene acceso al servicio de correo electrónico? ¿Podría su asistente enviarle por correo electrónico cualquier archivo que pudiera necesitar?”. Usted quizás podría considerar tomar este giro: una vez que haya reunido diferentes necesidades de acceso remoto en su compañía, trate que los usuarios escriban sus necesidades específicas. No solamente deberá obtener respuestas menos ambiguas, sino que también tendrá que reunir documentación importante que justifique los gastos requeridos y el esfuerzo en adquirir y configurar los sistemas de acceso remoto necesarios.

Cuando examine las necesidades de acceso remoto, debe estimar los requisitos de ancho de banda y las tolerancias de los diferentes usuarios. Esto es importante en la planeación y también para establecer las expectativas del usuario de forma adecuada. Por ejemplo, si el personal de ventas deseara tener acceso minuto a minuto al sistema de rastreo de ventas y también, de vez

en cuando, bajar paquetes de archivos de 4 MB para utilizarlos en sus cotizaciones, usted tendría que explicar las limitaciones de las velocidades de los módems y de las conexiones telefónicas a fin de limitar las expectativas de estos usuarios. O puede encontrar soluciones diferentes que satisfagan las necesidades de los usuarios y que sean coherentes con la cantidad de ancho de banda que pueda ofrecerles.

Usted puede estimar los requisitos de ancho de banda de algún programa de aplicación en particular de varias maneras. La primera involucra medir realmente las necesidades de ancho de banda de la aplicación. En la LAN, puede supervisar la cantidad de datos que se envían a un nodo en particular que utilice la aplicación en la forma que se utilizaría remotamente. Usted podría medir los datos de maneras diferentes. En una PC Windows, puede correr System Monitor o Performance Monitor en el cliente y observar el tráfico de la red que la PC consume (vea la figura 10-5). También puede medir el volumen de datos desde el servidor. En un servidor Windows NT o 2000, puede utilizar el Performance Monitor a fin de medir los bytes transmitidos hacia y desde el cliente. En un servidor Novell, puede utilizar la aplicación console Monitor para observar la cantidad de datos que se envían y reciben por medio de la conexión al servidor del cliente.

Si los requisitos de ancho de banda de una aplicación son demasiado grandes para ser manejados por el tipo de conexión remota que tenga disponible (como una conexión por módem a 33.6 Kbps), entonces necesita explorar otras alternativas. Dentro de éstas se incluye el uso de una solución de control remoto (analizada con mayor detalle en este capítulo), o bien, utilizar la aplicación de manera diferente. Por ejemplo, tal vez quiera cargar la aplicación en la computadora remota en lugar de utilizarla en la LAN. Asimismo, quizás las necesidades de datos del usuario no le demanden estar actualizado minuto a minuto, y pueda establecer un procedimiento por medio del cual el usuario reciba semanalmente actualizaciones de datos en un CD-ROM o mediante cualquier otro mecanismo.

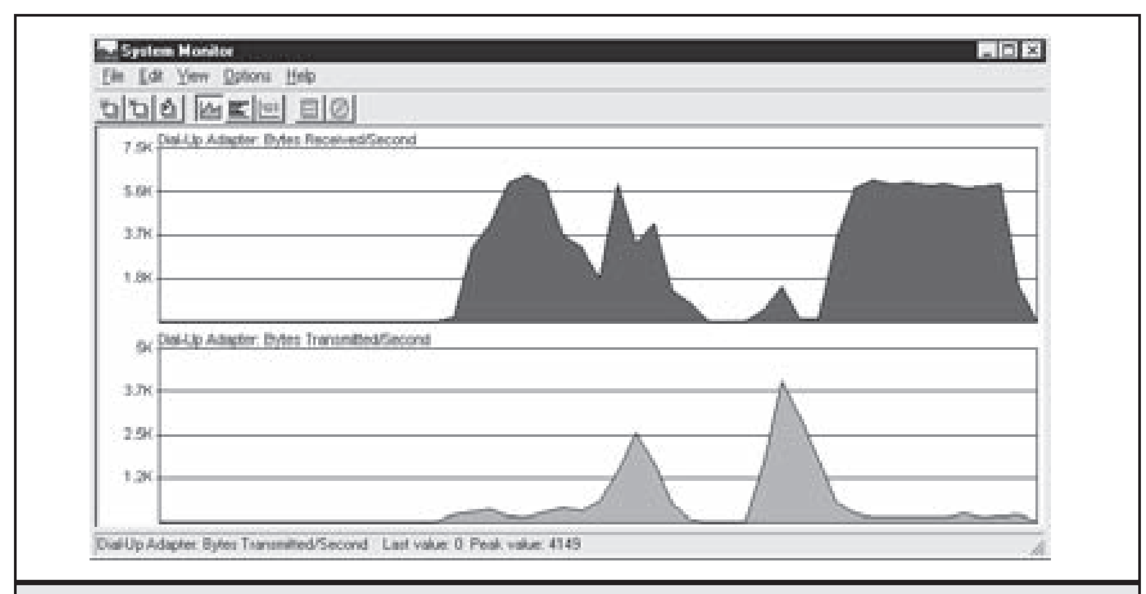


Figura 10-5. Utilización de Windows System Monitor para observar el ancho de banda que está utilizando una aplicación.

Las formas como puede satisfacer las necesidades de acceso remoto son virtualmente ilimitadas. Sin embargo, la clave está en el análisis cuidadoso de las necesidades y el trabajo creativo, considerando su tecnología de acceso remoto propuesto o disponible, con objeto de encontrar formas para satisfacer las necesidades de los usuarios remotos.

APRENDER LAS TECNOLOGÍAS DEL ACCESO REMOTO

Existe una gran variedad de formas de realizar conexiones de acceso remoto a los usuarios. A veces, estas tecnologías son adecuadas para algunos usuarios, pero no para todos. En ocasiones, las alternativas con las que usted cuenta están restringidas a la forma como el usuario remoto necesita acceder a los datos. Por ejemplo, un usuario remoto en un solo punto puede, con mucha facilidad, establecer un enlace de alta velocidad hacia la LAN corporativa, mientras que un usuario remoto que viaje puede estar limitado a utilizar conexiones por módem y líneas telefónicas conectadas a éste.

Las secciones siguientes analizan las diferentes técnicas y tecnologías, junto con las ventajas y desventajas de cada una. Las que usted implante dependerán de las necesidades que haya identificado, de su presupuesto y de la infraestructura existente en su red.

Nodo remoto en comparación con control remoto

Los usuarios remotos pueden conectarse a una red de dos formas básicas: por nodo remoto o por control remoto. Una *conexión de nodo remoto* es aquella en la que la computadora remota se convierte en un nodo de la red. Los datos fluyen entre el nodo remoto y la red de la misma forma en que lo haría con un usuario conectado a una LAN, aunque generalmente a velocidades más lentas. Cuando usted se conecta a un ISP para acceder a Internet, está utilizando una conexión a un nodo remoto.

Una *conexión a control remoto* es una en la que el usuario remoto toma el control de otra computadora que está directamente conectada a la LAN, solo con la información de la pantalla, el teclado y el ratón que se transmiten a través de la conexión. Debido a que la computadora del control remoto se encuentra directamente conectada a la LAN, su desempeño en la red es tan rápido como la de cualquier otra estación de trabajo de la LAN. La información que en realidad se transmite —la información de la pantalla y los datos del teclado y del ratón— generalmente no requiere mucho ancho de banda. (Una excepción de esta regla es una aplicación con alto contenido de gráficos, como el programa de dibujo CAD). Las conexiones de control remoto también pueden transferir archivos hacia adelante y hacia atrás de la computadora remota a la computadora controlada, por lo que los archivos pueden bajarse de la LAN a la computadora remota y viceversa.

El control remoto se obtiene mediante la utilización de aplicaciones especiales diseñadas para este propósito. Algunos ejemplos de software de control remoto son el PCAnywhere, Carbon Copy y ReachOut, así como Windows NT Terminal Server (o Terminal Services, para servidores Windows más recientes) y Citrix MetaFrame. Usted corre el software de control remoto en la computadora conectada a la LAN y en la computadora remota. La conexión se establece a través de una línea conmutada o Internet.

Dos tipos de aplicaciones de control remoto se encuentran disponibles. La primera corre en una sola computadora y soporta a la vez una sola computadora remota. PCAnywhere y Carbon Copy son ejemplos de este tipo. Otro, permite que se corran sesiones múltiples en una sola computadora, por lo que se puede tener a más de un usuario utilizando una sola computadora

conectada a la LAN; ejemplos de este tipo sonTerminal Server de Windows NT, Terminal Services de Windows y Citrix MetaFrame. Las soluciones multiusuario utilizan la capacidad de realizar varias tareas de la computadora LAN a fin de construir múltiples PC virtuales, ventanas y escritorios, como un tipo de computadora grande con sesiones terminales múltiples.

El control remoto es la mejor opción cuando los usuarios remotos necesitan tener acceso a las aplicaciones que no funcionan bien en conexiones de menor ancho de banda; y ya que la mayoría de las aplicaciones no corren bien a través de conexiones lentas, estos usuarios generalmente encontrarán que una aplicación conectada a una LAN trabaja mejor con el control remoto que con el nodo remoto.

Cualquier tecnología de conexión remota puede trabajar tanto con el nodo remoto como con el control remoto. Usted puede conectarse a un sistema de control remoto mediante módems conectados directamente a la computadora de control remoto, a través de líneas ISDN, Internet e incluso por medio de un enlace LAN o WAN.

¿Cómo sabe si debe escoger conexiones de nodo remoto o de control remoto? Considere estos puntos:

▼ Cuando un usuario remoto necesita solo acceso a archivos en la LAN y al correo electrónico, un nodo remoto puede satisfacer estas necesidades y, a menudo, es más fácil de configurar y mantener en ambos lados de la conexión.

■ Si un usuario remoto necesita correr una aplicación que esté conectada a la LAN, seleccione el control remoto. Pocas aplicaciones serán capaces de correr razonablemente bien a través de una conexión de nodo remoto, a menos que la aplicación se encuentre ya instalada en la computadora remota y ésta sólo accesará a pequeñas cantidades de datos a través del enlace remoto. Por ejemplo, el acceso al correo electrónico a través de Microsoft Outlook trabaja bien mediante una conexión de nodo remoto, siempre y cuando los usuarios remotos ya tengan este programa instalado en su computadora local.

■ Muchas aplicaciones en la actualidad están habilitadas para la web, de manera que un usuario remoto pueda emplear un navegador de web para tener acceso a ellas y utilizarlas. Estos tipos de aplicaciones corren igualmente bien —más o menos— a través de una conexión de nodo remoto o de control remoto. Por ejemplo, Microsoft Exchange Server soporta varios tipos de conexión, incluyendo el acceso web a bandejas de correo y calendarios, por medio de una característica llamada Web Outlook. Muchos sistemas de contabilidad cliente/servidor han comenzado a implantar el acceso a la web.

▲ Si necesita mantener una aplicación directamente para los usuarios, el control remoto podría ser la forma de proceder, ya que instala la aplicación en la máquina conectada a la LAN, desde donde usted puede accesar fácilmente para hacer cambios en la configuración o llevar a cabo cualesquiera otras acciones de mantenimiento. El usuario remoto corre solamente el software de control remoto y al instante se beneficia de cualquier trabajo que realice en la máquina conectada a la LAN. Esta capacidad puede ofrecer una ventaja real si sus usuarios de red no quieren reparar y dar mantenimiento al software. Con dicha conexión, usted puede manejar con mayor facilidad cualquier problema que se pueda presentar sin tener que viajar a algún lugar remoto o requerir que los usuarios le envíen sus computadoras para que las repare y les dé mantenimiento.

Ya sea que usted seleccione el nodo remoto o el control remoto, tendrá que determinar cómo se conectarán los usuarios a la LAN. Existen varias formas de llevar a cabo esta conexión, como se analizará en las secciones siguientes.

Módem o no módem, ésa es la pregunta . . .

Los usuarios remotos pueden tener acceso a su red de dos formas: conectándose a dispositivos que, a su vez, están conectados a la red de alguna forma; o conectándose a un ISP y, después, enlazarse con la red a través de una conexión de Internet de la LAN. Por ejemplo, los usuarios pueden utilizar un módem para marcar a otro conectado a la LAN que usted mantiene. De manera alternativa, los usuarios pueden utilizar un módem para conectarse a otro administrado por un ISP y, después, utilizar la conexión de Internet de la LAN para tener acceso a ésta.

Administre sus propios módems

En redes pequeñas, a menudo puede ser más fácil agregar un módem o dos a una computadora, para aceptar conexiones remotas y, después, dejar que los usuarios los usen para conectarse. Usted puede configurar los módems de las PC individuales que corran software de control remoto, en PC que corran software de nodo remoto (como el RAS de Windows NT) o en interfases especiales conectadas a la LAN, construidas con el propósito de ofrecer conexiones de nodo remoto. También puede construir su propia "granja de módems" con decenas o cientos de módems, utilizando un hardware especial que soporte estos usos.

Aproveche los módems de otros fabricantes

Generalmente, es un verdadero relajo que administre sus propios módems, ya que no solamente tiene que hacer esto, sino que también tiene que administrar el software y hardware del nodo remoto, las líneas telefónicas que se utilicen y todos los problemas que puedan presentarse en un momento dado. Si una LAN tiene ya un enlace de alta velocidad a Internet, como a través de un T-1 completo o fraccional, podría ser relativamente fácil dejar que los usuarios remotos marquen al ISP local y, después, se conecten a la LAN por medio de Internet. Dicho escenario tiene muchas ventajas:

- **No es necesario soportar módems directamente** Usted no tiene por qué preocuparse acerca de la administración de los módems. Si los usuarios no pueden conectarse, pueden llamar el ISP para solicitar ayuda. Los ISP más grandes cuentan con un grupo de soporte las 24 horas en el sitio con el fin de proporcionar ayuda, que implica que los llamen a las 2:00 a.m. porque un usuario en Europa no puede conectarse.
- **No se cobran tarifas de larga distancia** El usuario solo tiene que hacer una llamada local para conectarse con el ISP, lo que le permite ahorrar los costos de larga distancia en comparación con el marcado a la LAN directamente.
- **Impacto mínimo en el desempeño de la LAN** La utilización de la conexión a Internet a través de la LAN generalmente no afecta a los usuarios de ésta, quienes también utilizan esta conexión, por dos razones. Primero, muchos usuarios remotos se conectan a la LAN fuera de sus horas de trabajo cuando la conexión a Internet probablemente no se utiliza mucho. Segundo, debido a que el usuario remoto está conectado al ISP, generalmente a través de una conexión de módem lenta a 33.6 o 56 Kbps, el impacto total en su enlace de alta velocidad a Internet es mínimo, aun durante horas de trabajo.

- **Conexiones a alta velocidad** Sus usuarios pueden aprovechar cualquier enlace de alta velocidad a Internet que esté disponible para ellos y usted no tiene por qué preocuparse por tener que implantar tecnología de acoplamiento en el lado de la LAN. Un usuario puede utilizar una línea *x*DSL, un módem por cable o una línea ISDN y después conectarse a un ISP que soporte esa conexión de alta velocidad. Por el lado de la LAN, la conexión de alta velocidad (por ejemplo, un T-1) permanece igual.
- **Mejor acceso global** Los usuarios que viajan a otros países correrán con mejor suerte al tratar de conectarse a una ISP local que a través de una conexión telefónica internacional. La utilización de un módem de manera internacional es un poco problemática, pues las velocidades de conexión son bajas, la calidad de la línea no es buena y los retardos asociados con las conexiones por satélite (la mayor parte del tráfico telefónico internacional se da vía satélite) provocan problemas adicionales. Y, por supuesto, el costo puede ser prohibitivo. En una ocasión gasté cientos de dólares solamente revisando mi correo electrónico de Singapur a Estados Unidos varias veces en una semana, debido a que las tarifas telefónicas en ese país son más costosas que en Estados Unidos: las llamadas generadas desde Singapur en ese entonces costaban de dos a tres dólares el minuto (incluso la tarifa estándar de 0.75 centavos de dólar por minuto a Singapur hubiera sido cara). Una solución mucho mejor hubiera sido marcar a un módem ISP ubicado en el sitio (la mayoría de los ISP grandes como CompuServe o AT&T tienen presencia en casi todos los países) y emplear Internet para conectarme a la LAN en Estados Unidos. Dicha solución hubiera sido más barata, confiable y rápida. (Sin embargo, entonces este tipo de conexiones no eran factibles como lo son ahora).

Cuando permite que los usuarios remotos accedan a la LAN a través de Internet, generalmente emplea una tecnología llamada conectividad de redes privadas virtuales (virtual private networking, VPN), la cual consiste en un enlace de red entre el usuario remoto conectado a un ISP y la LAN de la compañía a través de Internet. Las redes privadas virtuales utilizan un encriptado de paquetes muy sofisticado y otras tecnologías, por lo que el enlace desde el usuario a la LAN es seguro, a pesar de que se transporte por una red pública. Las soluciones VPN varían desde las más simples que pueden implantarse en un Servidor de Windows prácticamente sin costo (utilizando el servicio RAS, incluido con Windows NT Server o el servicio equivalente, RRAS, en Windows 2000 o Windows Server 2003) hasta los ruteadores VPN especializados e independientes que pueden soportar a cientos de usuarios. La figura 10-6 muestra cómo trabaja una conexión VPN.



PISTA Windows 98 y Windows Me incluyen soporte integrado para conexiones VPN del lado cliente. Usted también puede obtener soporte para Windows 95 bajando la versión 1.3 (o posterior) del software de conectividad de redes conmutadas de Windows 95. Asimismo, muchos fabricantes de ruteadores VPN independientes le permiten obtener licencias del software VPN para los usuarios remotos. Algunos fabricantes cobran una cuota por cada licencia del software, mientras que otros incluyen una licencia para un número ilimitado de usuarios remotos como parte de su ruteador VPN.

Enlaces remotos a velocidades más elevadas

Las conexiones por módem son muy lentas, en general corren a 33.6 Kbps. Aunque muchas aplicaciones pueden diseñarse para que trabajen razonablemente bien a esta velocidad de conexión, la tendencia es que esta velocidad se está haciendo inapropiada, incluso si solo se emplea para

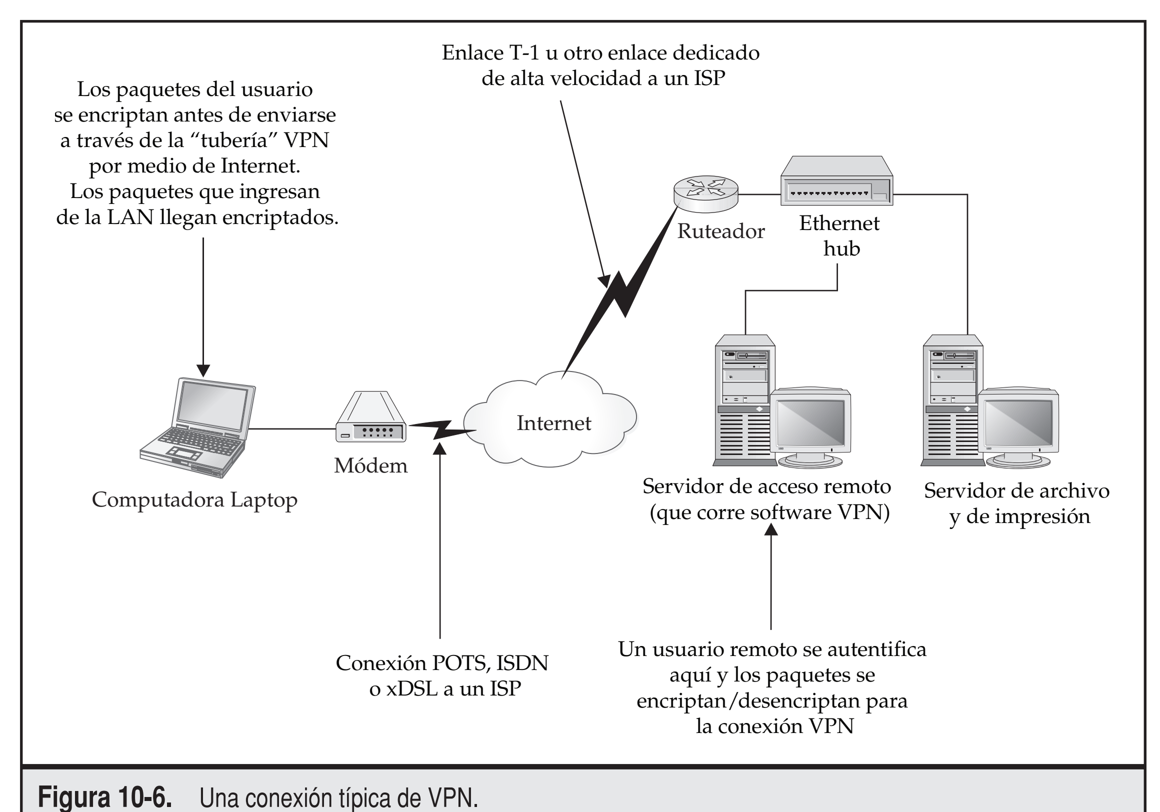


Figura 10-6. Una conexión típica de VPN.

transferir archivos. (Aparentemente, los archivos de aplicaciones siguen aumentando con cada nueva versión).

Sin embargo, los módems son todavía el medio más usual de acceso remoto, ya que las conexiones estándar POTS (servicio telefónico convencional) están disponibles virtualmente en todas partes y los módems trabajan razonablemente bien, considerando todos los aspectos.

PISTA Los módems disponibles en estos días funcionan a velocidades de hasta 56 Kbps. Sin embargo, existe una desventaja en esta característica: requiere que el otro extremo de la conexión cuente con una conexión digital. Además, la capacidad de 56 Kbps es una velocidad máxima disponible en la dirección hacia abajo; en la dirección hacia arriba nunca excede los 33.6 Kbps, aun cuando está conectado a un ISP que utilice conexiones digitales capaces de manejar 56 Kbps en su extremo. Usted no tendrá 56 Kbps a través de líneas telefónicas estándar, incluso si ha acoplado módems a 56 Kbps en ambos extremos; la velocidad máxima que obtendrá será de 33.6 Kbps en ambas direcciones a través de líneas telefónicas convencionales con módems estándares en cada extremo.

En pocas palabras, los usuarios que viajan a diferentes puntos necesitan depender de conexiones vía módem. No existe todavía una conexión de suficiente ancho de banda como para que se pueda tener acceso en la mayoría de los hoteles, aunque esta situación está mejorando rá-

pidamente y ahora muchos hoteles ya cuentan con puertos de acceso a Internet de alta velocidad en sus habitaciones. Sin embargo, se ha dicho que las líneas telefónicas y los módems son todavía el mínimo común denominador del que pueda depender. No obstante, las conexiones a alta velocidad son muy factibles para los usuarios remotos que se encuentran en un solo punto. Los usuarios caseros en muchas áreas metropolitanas pueden ahora obtener DSL de alta velocidad y conexiones con módem por cable a Internet. Y se pueden beneficiar de estas altas velocidades cuando se conectan a las LAN corporativas si usan un VPN. Incluso para quienes no tengan DSL o módems por cable disponibles en su área, generalmente el ISDN de la compañía telefónica local es una opción.

Los usuarios remotos que utilizan DSL o módem por cable están conectados físicamente a un ISP en particular en su conexión, por lo que tienen que utilizar una forma de VPN para conectarse a la LAN. Por otro lado, los usuarios de ISDN tienen la opción de conectarse a un ISP con capacidad de ISDN o a "módems" ISDN ubicados en la LAN. Mediante un proceso llamado *enlazado*, los usuarios de ISDN pueden alcanzar velocidades de hasta 128 Kbps, aunque esto consume dos canales B (¡y duplica la tarifa de las llamadas!). Con todo y eso, dichas velocidades son más atractivas que los 33.6 Kbps que puede alcanzar por medio de un módem.



NOTA Las tecnologías ISDN y DSL se estudian con más detalle en el capítulo 7.

Redes privadas virtuales

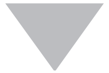
En este capítulo ya se mencionaron las VPN, sin embargo, su importancia en el acceso remoto amerita dedicarles una sección a fin de explorarlas más a fondo. VPN es una tecnología de gran importancia que se está utilizando de manera muy amplia. Una conexión a una red VPN se lleva a cabo a través de una red compartida o pública —la cual casi siempre es Internet— y encripta los datos para que solo el cliente y el servidor de VPN puedan leerlo. Las conexiones VPN cuestan mucho menos que las conexiones dedicadas, como las tecnologías WAN analizadas en el capítulo 7, ya que éstas aprovechan las eficiencias del costo del Internet sin comprometer la seguridad.

Las conexiones VPN se utilizan de dos formas importantes:

▼ Para formar conexiones WAN utilizando tecnología VPN entre dos redes que puedan estar a miles de kilómetros de distancia, pero que cada una tenga alguna forma de acceder a Internet.

▲ Para formar las conexiones de acceso remoto que permitan a los usuarios remotos acceder a la LAN a través de Internet.

La importancia de este capítulo radica en el acceso remoto; sin embargo, es importante saber que los VPN soportan las conexiones WAN de forma muy similar a como soportan una conexión de acceso remoto. La diferencia principal de una conexión de WAN VPN es que ésta conecta dos redes, en lugar de conectar a un usuario y una red, y depende de hardware diferente (por lo general) al que utiliza una conexión de acceso remoto. Una conexión VPN WAN aprovecha la conexión existente a Internet para ambas LAN y puede operar virtualmente las 24 horas del día. Una conexión de acceso remoto, por otro lado, es común que se forme cuando se necesite y utiliza hardware menos costoso por el lado remoto, como un módem de marcado o, quizás, una conexión de alta velocidad a Internet, como xDSL, ISDN o cable módem.



PISTA En algunas circunstancias, una VPN puede ser aún una forma apropiada de segregar usuarios en una sola ubicación de otros usuarios, utilizando la intranet de la compañía para almacenar el túnel VPN. Por ejemplo, dicho esquema puede ser el adecuado si un grupo de usuarios tiene acceso a datos que sean tan sensibles que deban estar separados del resto de la compañía de alguna forma. Entonces, la red sensible puede estar separada de una LAN corporativa, excepto por una pared que permita las conexiones VPN de la LAN sensible a la LAN corporativa, pero no al revés. Además, esta configuración permite que los usuarios en la LAN sensible puedan tener acceso a los servicios generales de la red corporativa.

Protocolos VPN

Una conexión VPN tiene varios requisitos. Primero, ambos lados de la conexión VPN deben estar conectados a Internet, generalmente utilizando el protocolo punto a punto (PPP). (Otras redes públicas o privadas pueden también transportar VPN; sin embargo, este tema se relaciona con Internet, ya que es la red que se utiliza con mayor frecuencia para este propósito). Segundo, ambos lados deben tener un protocolo de conectividad en común, el cual es generalmente, TCP/IP, sin embargo, puede ser también IPX, NetBEUI o AppleTalk. Tercero, ambos lados deben establecer un *túnel* a través de sus conexiones PPP existentes, mediante las cuales, circularán sus paquetes de datos. El túnel se forma utilizando un *protocolo de túnel*. Por último, ambos lados deben estar de acuerdo con la técnica de encriptado por utilizar con los datos que circulen por el túnel. Una gran variedad de técnicas de encriptado se encuentran disponibles.

Los tres protocolos de túnel más populares que se utilizan en las VPN son: protocolo de túnel punto a punto (PPP), protocolo de túnel de la capa dos (L2TP) y la seguridad del protocolo de Internet (IPSec). El PPTP es un protocolo diseñado por Microsoft que puede manejar paquetes IP, IPX, NetBEUI y AppleTalk. El PPTP está incluido en las versiones actuales de Windows, a partir de la Windows 95, y también está soportado por el Servicio de Acceso Remoto y Enrutamiento de Windows NT (RRAS, una actualización sin costo del Servicio de Acceso Remoto) y por Windows 2000 y Windows Server 2003. Para una red orientada a Windows, PPTP es la forma de proceder. L2TP es un protocolo más nuevo que es un estándar de la Fuerza de Tarea de Ingeniería de Internet y, probablemente, se convertirá en el protocolo túnel más ampliamente soportado, ya que opera en la capa dos del Modelo OSI y, por tanto, puede manejar todos los protocolos de la capa tres, como el IP, IPX o AppleTalk. El IPSec es tal vez el protocolo túnel más seguro y parece ser más popular para las VPN LAN a LAN y para las VPN orientadas a UNIX, debido a su dependencia de IP. El IPSec es un protocolo de la capa tres y está limitado al manejo del tráfico IP solamente.



PISTA Mientras IPSec trabaja solamente con paquetes de IP, una VPN L2TP también puede transportar los paquetes IPSec resultantes, ya que éstos pueden manejarse de la misma forma que los demás paquetes de la capa tres, como los paquetes IP, IPX y AppleTalk.

Tipos de VPN

En la actualidad, se utilizan cuatro tipos principales de VPN. El primer tipo utiliza un ruteador con capacidades VPN adicionales. Los ruteadores VPN no solo pueden manejar tareas de enrutamiento normal, sino que también pueden configurarse para formar VPN a través de Internet a los demás ruteadores similares, ubicados en redes remotas. Este método se utiliza para crear enlaces WAN VPN sobre Internet, generalmente entre múltiples edificios de una compañía.

El segundo tipo principal de VPN es el que se encuentra integrado a un firewall. Los firewall más importantes, como la Firewall-1 de CheckPoint o la Firebox de Watchguard, no solamente sirven como dispositivos de pared, sino que también sirven como hosts de VPN. Las VPN de pared se pueden utilizar tanto para soportar a usuarios remotos como también para proporcionar enlaces VPN de WAN. El beneficio de utilizar un VPN basado en firewall es que usted puede administrar su seguridad en la red, incluyendo la del firewall estándar como la VPN, totalmente dentro del firewall. (Por ejemplo, puede configurar el firewall a fin de permitir conexiones a la red solo cuando se realicen como parte de una conexión VPN válida).

El tercer tipo principal de VPN incluye aquellas que se ofrecen como parte de una sistema operativo de red. Los mejores ejemplos de este tipo son el RRAS de Windows NT, el Windows 2000 y NetWare 5 que corre con el software BorderManager de Novell. Estas VPN se utilizan con mayor frecuencia para soportar el acceso remoto y son generalmente las menos costosas de adquirir e instalar. (En el caso de Windows NT y Windows 2000, el NOS incluye los servicios de VPN).

El cuarto tipo principal es el VPN SSL. Éste es, en realidad, mi favorito para el soporte al acceso remoto y se estudia en una sección más adelante en este capítulo.

Clientes VPN

A ambos lados de una conexión VPN debe correr software compatible con VPN, que utilice protocolos compatibles. Para una solución VPN de acceso remoto, el software que instale depende de la VPN en sí. Las soluciones VPN dedicadas también venden software del cliente que usted puede distribuir a sus usuarios que, en general, tiene un cargo por copia que va de 25 a 50 dólares por computadora remota soportada. (Algunas VPN incluyen licencias ilimitadas para clientes, sin embargo, la VPN tiene licencia para aceptar solamente un cierto número de conexiones al mismo tiempo).

Si está utilizando un servidor Windows y un servicio RRAS en el servidor, y alguna versión de Windows 95 o posterior en la computadora remota, entonces puede aprovechar el software VPN incluido sin costo con esos sistemas operativos. Sin embargo, este software debe aún configurarse en cada computadora del cliente.

VPN SSL

Como mencioné antes, mi tipo favorito de VPN para soportar el acceso remoto es el VPN SSL, una categoría de producto que surgió en el último par de años. Una VPN SSL aprovecha la tecnología de encriptado de la Capa Socket de Seguridad incluida en la mayoría de los navegadores de la web para ofrecer los servicios de VPN a través de éstos. SSL es la misma tecnología que se utiliza en el encriptado de información de las páginas web que utiliza el prefijo **https://** como en los sitios web de banca en línea o sitios comerciales.

Existen un gran número de beneficios que las VPN SSL ofrecen para soportar el acceso remoto:

- No es necesario instalar ningún software de cliente en la computadora remota, excepto por una adición de ActiveX o Java que se instala en el navegador de manera automática.
- No se necesita, en esencia, ninguna configuración o administración en el sistema remoto. Éste es un punto importante, ya que la mayoría del software del cliente VPN es muy difícil de soportar.

- Si los usuarios conocen la dirección web del servidor VPN SSL y cuentan con la información correcta para autentificarse (firmarse) en el sistema, pueden hacerlo desde casi cualquier computadora conectada a Internet en el mundo y acceder a una amplia gama de servicios de red a través de simples páginas web.
- Debido a que muchas funciones comunes, como la administración de archivos, pueden llevarse a cabo utilizando páginas web, las VPN SSL funcionan mucho mejor a través de conexiones de menor ancho de banda que otras alternativas de VPN. HTML fue diseñado para ser "tacaño" en el uso del ancho de banda de la red, y muchas tareas que son lentas a través de una conexión VPN tradicional son más rápidas con un VPN SSL.
- La mayoría de las VPN SSL, además de sus características de acceso basado en la web, también permiten que el usuario comience una conexión al nodo remoto por demanda, la cual funciona automáticamente instalando y configurando plug-ins al navegador.

Las VPN SSL se ofrecen, típicamente, como un aparato doméstico: una pieza de equipo instalada en estantes que contiene todo el hardware y software necesarios para operar la VPN SSL. Esto da pie a la única desventaja real de las VPN SSL: son muy caras para compañías pequeñas, pues las configuraciones más pequeñas van de 8 000 a 10 000 dólares y soportan hasta 100 usuarios simultáneos. Sin embargo, aun si solo tiene que soportar de 20 a 30 usuarios remotos, encontrará que éste es un precio bajo si considera la reducción de trámites administrativos de una VPN tradicional, los cuales son a menudo muy cuantiosos.

En el momento de la escritura de este libro, existen muchos proveedores de VPN SSL. El pionero en este campo es la familia de productos Netscreen de Juniper Networks, que adquirió un producto originalmente lanzado por una compañía llamada Neoteris, que en realidad fue el pionero de las VPN SSL. Otro líder es la línea de productos Firepass de F5 Networks. Otras firmas líderes que ofrecen VPN SSL incluyen AEP Networks, Aventail, Whale Communications y Nokia. Puesto que esta área de productos está evolucionando muy rápido, es recomendable que usted lleve a cabo una búsqueda muy cuidadosa de productos que satisfagan sus necesidades.

VPN SSL: una perspectiva del usuario

Para darle una idea de cómo una VPN SSL ve a un usuario de acceso remoto, se muestran en esta sección unas pantallas como ejemplo de una versión de demostración del Firepass 4000 de F5 Networks. La figura 10-7 muestra una pantalla típica después de navegar a la URL de las VPN SL. (Si usted emplea una VPN SSL, esta pantalla presentaría el logo de su compañía y otra información).

Las VPN SSL pueden autentificar a los usuarios que utilicen una gran variedad de técnicas diferentes, incluyendo las siguientes:

- Por medio de los nombres y contraseñas de usuarios definidos en la VPN SSL de cada usuario.
- Mediante la integración con el sistema de autentificación existente, como el Windows Active Directory. La selección de esta opción, por ejemplo, permite que los usuarios remotos utilicen su nombre y contraseña normal de usuario de red y, entonces, la VPN SSL se integra con el sistema de autentificación preexistente en la red.



Figura 10-7. Una pantalla de ingreso a una VPN SSL.

- ▲ Por medio de la integración de un sistema de autentificación del factor 2 el cual, por lo general, incluye un pequeño dispositivo para cada usuario que despliega una gran cantidad de cambios cada minuto o algo así. Los usuarios se firman tecleando el número en el dispositivo, más un número adicional que solo ellos conocen (algo parecido al número de PIN de un cajero automático). Los sistemas de autentificación de factor 2 son extremadamente seguros, ya que los dispositivos utilizan una secuencia aleatoria de números que solamente los conoce un servidor de seguridad instalado en la red.

Una vez que los usuarios se firman en una VPN SSL, se les muestra una página de inicio que despliega todas las opciones de conexión que tienen disponibles, como el ejemplo que se muestra en la figura 10-8. Los tipos de alternativas disponibles para un usuario remoto pueden incluir los siguientes:

- ▼ Acceso a una conexión de nodo remoto a través de una VPN SSL.
- ■ Acceso a otros servidores web en la red de la compañía, como un sitio intranet corporativo que no es accesible a través de Internet.

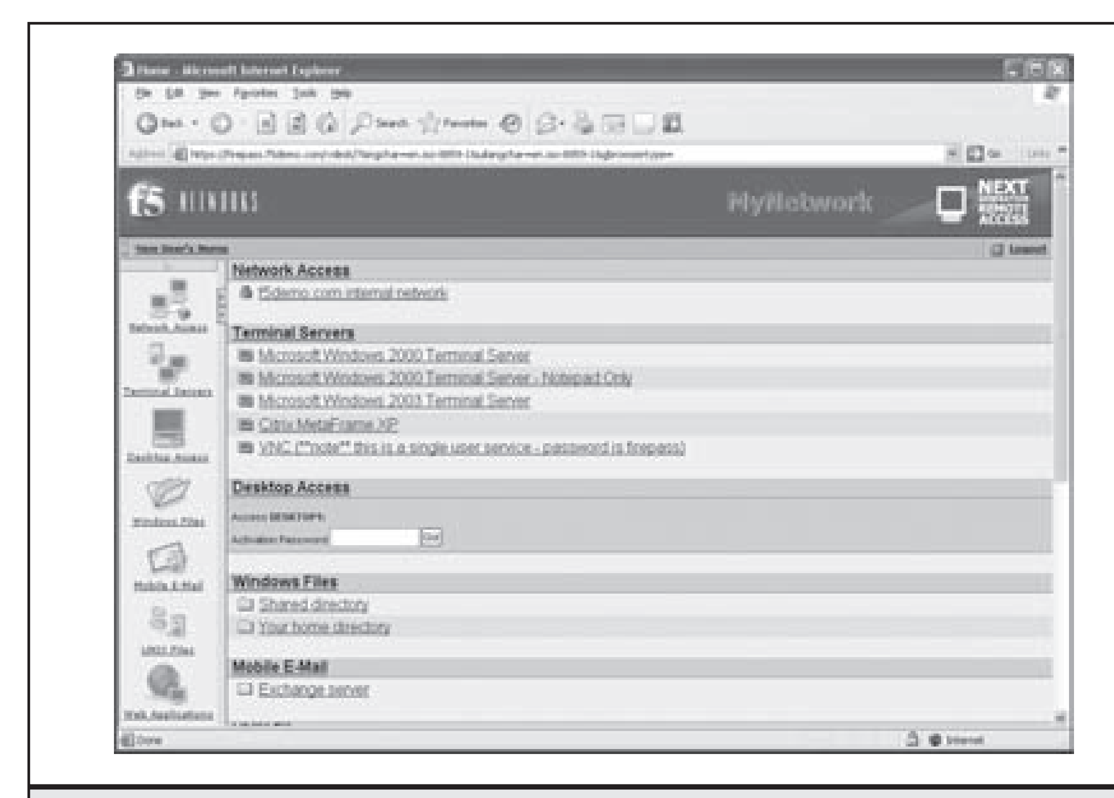


Figura 10-8. Ejemplo de una página de inicio de usuario en la VPN SSL.

- Acceso a correo electrónico, ya sea a través de algo como Web Outlook o a través de un cliente de correo electrónico habilitado por la web proporcionado por la VPN SSL.
- La capacidad de llevar a cabo la administración de archivos basada en el web a través de la VPN SSL. Los archivos administrados deben estar almacenados en servidores basados en Windows o Unix.
- Acceso a aplicaciones corporativas compartidas que han sido configuradas para trabajar a través de la VPN SSL, como un sistema de contabilidad.
- Acceso a sesiones Windows Terminal Services o Citrix vía la VPN SSL.
- Acceso a sesiones terminales de la computadora grande (mainframe).

Mientras que muchas de estas opciones son importantes en un gran número de compañías, la función principal del acceso remoto es dejar que los usuarios accedan al correo electrónico y a los archivos almacenados en la red. Como se mencionó anteriormente en este capítulo, las VPN SSL ofrecen un acceso basado en la web a muchos tipos diferentes de servidores de correo electrónico. También incluyen la habilidad de administrar archivos y directorios a través de una

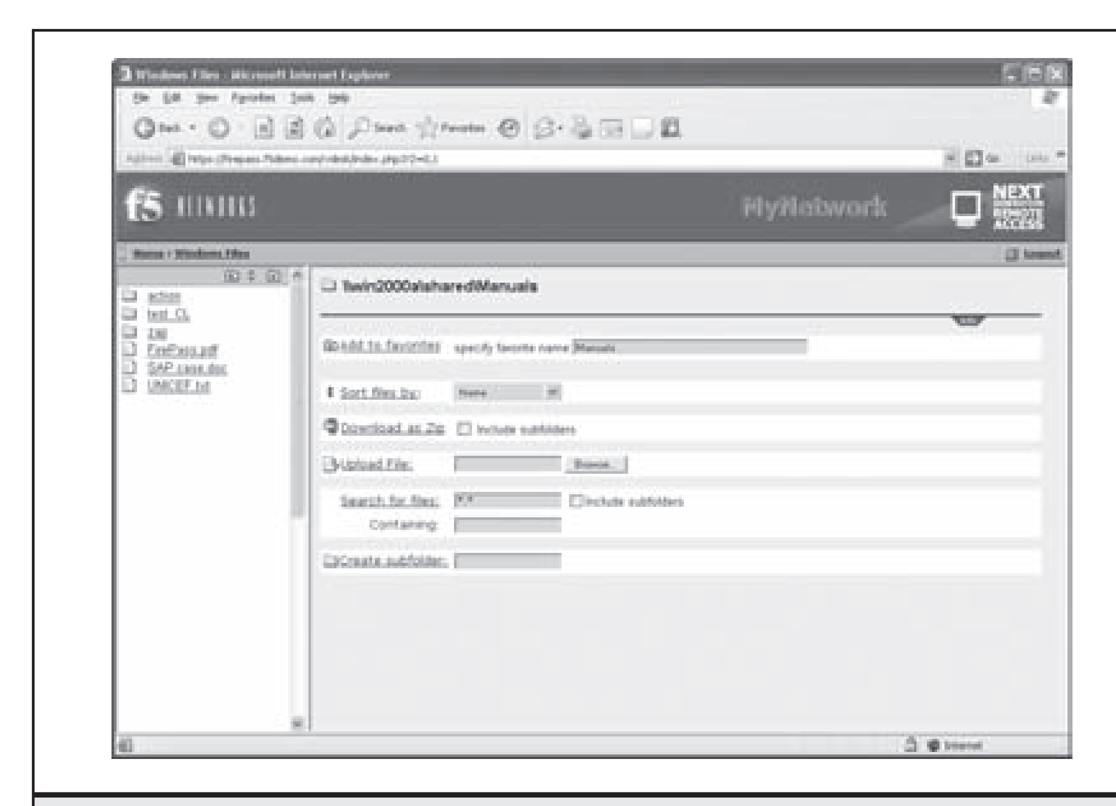


Figura 10-9. Carpeta que contiene algunos archivos que pueden administrarse.

interfase web, como la que se muestra en la figura 10-9. En este ejemplo, el usuario puede seleccionar archivos en la sección izquierda y después seleccionar bajar, agregar a un carrito para bajar software, ver dentro del navegador web, renombrar, o más aún, eliminar archivos. El usuario también puede administrar carpetas y subir archivos nuevos. Todo acceso a los archivos cuenta con permisos de red proporcionados al usuario que está firmado en la VPN SSL.

RESUMEN DEL CAPÍTULO

La mayoría de los administradores de red estarán de acuerdo con que soportar el acceso remoto es una de las partes más truculentas de la administración de cualquier red. Muchos factores se unen para dar como resultado lo anterior. Usted puede soportar conexiones remotas en un gran número de formas: la mayoría de las velocidades de conexión remota tiene un ancho de banda menor que el que quisieran los usuarios remotos; muchos usuarios son a menudo, personal de alto nivel en la empresa que tienen varios problemas en cualquier conexión realizada a larga distancia. Aun así, el acceso remoto es un servicio importante de red y los beneficios que brinda a la compañía justifican todos los esfuerzos que se hagan a cualquier nivel, que estén orientados a hacerlo confiable y que funcione como deba ser.

Utilice la información que aprendió para analizar las necesidades de acceso remoto de su empresa, para aprender qué necesitan sus usuarios en realidad y para comenzar a buscar, entre las diferentes soluciones posibles, las que más tengan sentido para su situación en particular. Usted deberá considerar también si necesita soportar más de un tipo de solución. Por ejemplo, la mayoría de las redes soportan tanto módems ubicados en la compañía como otros tipos de conexiones que viajen a través de un enlace VPN o puede soportar una solución de acceso remoto existente por un tiempo mientras instala algún tipo de solución VPN, además, puede decidir operar ambos sistemas por algún tiempo a fin de satisfacer sus necesidades específicas.

El siguiente capítulo trata acerca de las tecnologías y técnicas que mantienen la información de la red segura y alejada de malos manejos. La administración de la seguridad de la red, cuando se hace bien, no debe consumir mucho tiempo. Usted necesita invertir tiempo y esfuerzo suficientes cuando instale una red a fin de asegurarse de que la seguridad de ésta sea robusta desde el principio.

CAPÍTULO 11

Asegurando su red

Gran parte de las cosas que aprendió acerca de la conectividad de redes es relativamente directa, sin rodeos y usted puede realizarla. ¿Desea un nuevo archivo y un servidor de impresión? Usted lo instala, lo configura y puede funcionar o no. Si no funciona, procede a repararlo, arregla algunos problemas y, al final, acaba la tarea. Por otra parte, la seguridad de la red es algo muy diferente. De hecho, usted *nunca* puede terminar el proyecto de asegurar una red y *nunca* puede estar completamente seguro de que está segura. No importa cuánto dinero invierta en asegurar una red, cuánto tiempo dedica a esta tarea o cuánto hardware y software de seguridad instale: ninguna red está segura por completo. (Existe un corolario muy gracioso respecto a esto: La única red completamente segura es la que nadie puede usar).

Una vez dicho esto, la seguridad de la red es una de las tareas más importantes con la que tiene que lidiar un administrador. Una buena seguridad en la red ayuda a evitar lo siguiente:

- Que secretos empresariales, como diseños y procesos propietarios, caigan en malas manos (tanto internas como externas).
- Que la información personal acerca de sus empleados llegue a extraños.
- Que se pierda información importante y software.
- Que se inutilice la red en sí o cualquier parte de ella.
- Que se corrompa o modifique de forma inadecuada información importante.

¡DEFÍNALO! Dispositivos importantes de seguridad de redes

Aquí se mencionan algunos dispositivos importantes de seguridad de redes con los que usted debe estar familiarizado:

- **Firewall** Un sistema que promueve la política de seguridad entre dos redes, como una LAN e Internet. Los firewalls pueden utilizar muchas técnicas diferentes para promover las políticas de seguridad.
- **Servidor proxy** Un servidor que actúa como un proxy (un intermediario anónimo), generalmente para los usuarios de una red. Por ejemplo, puede existir un proxy para navegar por las páginas web, de forma que la computadora del usuario no tenga que estar conectada al sistema remoto, excepto a través del servidor proxy. En el proceso de dar acceso proxy a las páginas web, un servidor proxy también puede acelerar el acceso a la web al almacenar las páginas web que se accesan, de forma que los demás usuarios se beneficien de contar con ellas de manera más rápida desde el servidor proxy local; además puede ofrecer alguna protección de firewall a la LAN.
- **Filtro de paquetes** Generalmente construido en un ruteador o una firewall, un filtro de paquetes le permite fijarse un criterio para aceptar o no paquetes, direcciones IP de origen y destino, y puertos IP.

Lo anterior es una lista de algunos aspectos más importantes que puede evitar la seguridad de la red. Si usted se pone a pensar acerca de toda la información que se almacena y fluye a través de las redes en las que trabaja (y de hecho, debe invertir tiempo en pensarlo), probablemente encontrará otros daños adicionales que puede evitar.

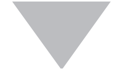
Este capítulo lo introduce en el tema de la seguridad de las redes. Su objetivo es familiarizarlo con ideas y conceptos importantes en relación con la seguridad y con varias tecnologías involucradas en este tema. Si usted es responsable de la seguridad de la red, deberá conseguir información más detallada y pensar seriamente en contratar a un especialista en la materia, a fin de que le ayude a asegurar su red, la seguridad de ésta es trabajo de todos; o bien, si es un profesional en sistemas de información, este tema es una parte muy importante de su trabajo.

COMPRENDER LA SEGURIDAD INTERNA

La *seguridad interna* es el proceso de asegurar su red contra amenazas internas, las cuales son, en general, mucho más comunes que las externas. Algunos ejemplos comunes de amenazas internas son los siguientes:

- Usuarios internos acceden, de forma inadecuada, a información a la que no deberían tener acceso, como los registros de nómina, los registros de contabilidad o la información sobre el desarrollo del negocio.
- Usuarios internos entran a los archivos de otros usuarios a los que no debieran tener acceso.
- Usuarios internos se hacen pasar por otros usuarios y provocan daños, como el envío de correos electrónicos con el nombre de otra persona.
- Usuarios internos se introducen en sistemas a fin de llevar a cabo actividades criminales, como desvío de fondos.
- Usuarios internos que comprometen la seguridad de la red, por ejemplo, al introducir accidentalmente (o deliberadamente) virus a la red. (Los virus se estudian en una sección independiente, más adelante en este capítulo).
- Usuarios internos "husmean" paquetes en la red a fin de descubrir cuentas de usuario y contraseñas.

Para lidiar con amenazas como éstas, necesita administrar la seguridad de la red en forma diligente. Debe suponer que, dentro de la población de usuarios internos, hay algunos que tienen el conocimiento y la curiosidad necesarios para explorar los agujeros de seguridad de la red y que, al menos algunos de ellos, hasta cierto punto, tienen una buena razón para hacerlo.



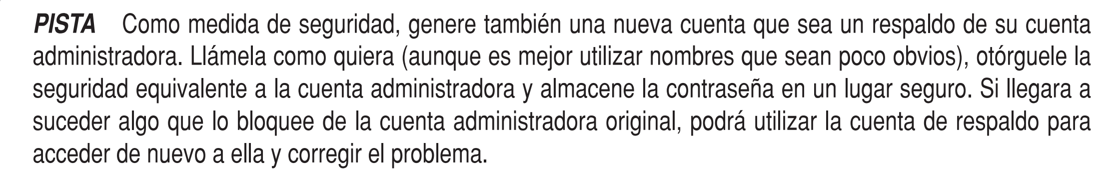
NOTA Una de las partes más desagradables de la administración de la seguridad es que es necesario que usted piense lo peor de la gente para que, en consecuencia, tome las medidas para prevenir esas acciones. En otras palabras, se requiere cierta cantidad de paranoia saludable. No es un estado mental agradable; sin embargo, se requiere hacer un buen trabajo en el campo de la seguridad. Recuerde también que obtendrá mejores resultados si contrata a una empresa para que le ayude a administrar la seguridad de la red, la

cual no solo tendrá un nivel mayor de habilidad en esta área, sino que su personal estará acostumbrado a pensar en torno a la seguridad y, de seguro, tendrán una amplia experiencia en la resolución de problemas de seguridad, forjada en otras compañías. Quizá más importante, el contratar a una empresa externa no pondrá a los empleados de seguridad en una posición de adversidad hacia sus compañeros.

Seguridad de las cuentas

La *seguridad de las cuentas* se refiere al proceso de administrar las cuentas de usuario habilitadas en la red. Se requiere una gran cantidad de tareas para administrar las cuentas de usuario de manera adecuada, además de que éstas deben ser auditadas periódicamente (de preferencia por una persona diferente a la que las administra diario), a fin de asegurarse de que no existan discrepancias. A continuación se listan varios pasos que debe tomar a fin de administrar la seguridad general de las cuentas:

- La mayoría de los sistemas de operación de red (network operating system, NOS) comienza con una cuenta de usuario llamada "Guest". Debe quitar esta cuenta de inmediato, ya que es el objetivo principal de los crackers. También debe evitar crear cuentas que tengan propósitos de prueba, como "Test", "Generis", etcétera.
- La mayoría de los NOS comienzan con un nombre predeterminado de la cuenta que administra el sistema. En los sistemas operativos Windows Server, la cuenta se llama Administrator; en NetWare, se llama Supervisor o Admin (dependiendo de qué versión esté usando). Usted debe renombrar de inmediato esta cuenta a fin de evitar ataques directos contra ella. (En NetWare 3.x, usted no puede renombrar la cuenta del Supervisor).


PISTA Como medida de seguridad, genere también una nueva cuenta que sea un respaldo de su cuenta administradora. Llámela como quiera (aunque es mejor utilizar nombres que sean poco obvios), otórguele la seguridad equivalente a la cuenta administradora y almacene la contraseña en un lugar seguro. Si llegara a suceder algo que lo bloquee de la cuenta administradora original, podrá utilizar la cuenta de respaldo para acceder de nuevo a ella y corregir el problema.

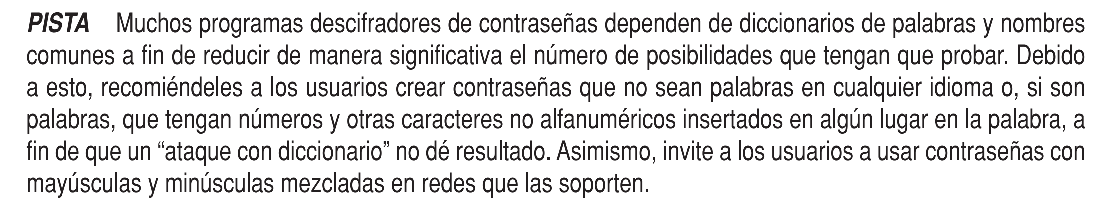
- Usted debe conocer los pasos que se requieren para eliminar, de manera rápida, el acceso a los recursos de la red desde cualquier cuenta de usuario y asegurarse de explorar *todos* los recursos de la red que puedan contener sus propios sistemas de seguridad. Por ejemplo, las cuentas se administrarán en el NOS (y después en cada servidor) y también en aplicaciones específicas como los servidores de bases de datos y sistemas de contabilidad. Asegúrese de que descubrirá cómo maneja el sistema las cuentas eliminadas o desactivadas. Si elimina una cuenta de usuario con la finalidad de quitar el acceso, algunos sistemas, en realidad, no niegan el acceso a ese usuario hasta que finalice su sesión en el sistema.
- Trabaje en conjunto con el departamento de recursos humanos, a fin de que sea confortable trabajar con usted en el manejo de asuntos de seguridad relacionados con la salida de empleados, además desarrolle una lista estándar de verificación para asentar los cambios de personal relacionados con el departamento de recursos humanos que afecten al departamento de tecnología de la información (TI). Es probable que este departamento no pueda avisarle con anticipación; sin embargo, debe comprender que usted requiere saber acerca de cualquier renuncia o despido de manera *inmediata*, a fin

de que pueda tomar las medidas apropiadas. Siguiendo la misma línea, usted querrá diseñar un conjunto de procedimientos acerca de cómo manejar los correos electrónicos acumulados, los archivos y cualquier otro acceso del usuario tanto en despidos como en renuncias amistosas. Su relación con la gente adecuada del departamento de recursos humanos es crucial para administrar la seguridad de manera satisfactoria, por lo que deberá asegurarse de fomentar y conservar una confianza mutua.

- Considere la instalación de un programa por medio del cual el supervisor pueda revisar los permisos asignados y autorizados de los usuarios nuevos en la red. De esta forma, será casi imposible que, por error, usted otorgue el acceso a un usuario a cosas que él o ella no estén autorizados a ver.
- Para las compañías que cotizan en la bolsa de valores, la entrada en vigor de la Ley Sarbanes-Oxley de 2002 implica que tal vez usted tenga que instalar un sistema a fin de documentar cómo se agregan, modifican y eliminan los usuarios del sistema. Este tipo de sistema, generalmente, involucra que el departamento apropiado (recursos humanos, contabilidad, etc.) solicite que se llene una serie de formatos de solicitud, firmados por el supervisor individual y otras instancias que necesitan autorizar el acceso a ciertos sistemas y después documentar las acciones del grupo de tecnologías de la información. Posteriormente, estos formatos se archivan para que puedan ser examinados por los auditores de la compañía en cualquier momento.

Otro aspecto importante de la seguridad de las cuentas es la seguridad de sus contraseñas. La mayoría de los NOS le permite establecer políticas en relación con la seguridad de las contraseñas, las cuales controlan la frecuencia con que el sistema obliga a los usuarios a cambiarlas, el periodo de validez de éstas, si es posible que los usuarios puedan reutilizar una ya usada con anterioridad, entre otros aspectos. Por lo menos, tome en cuenta las siguientes sugerencias para establecer las políticas de las contraseñas:

- Debe solicitar a los usuarios (por medio de los lineamientos de la política de contraseñas de la red) que cambien su contraseña a la red principal cada 90 a 180 días. (30 días es una recomendación muy común, sin embargo, en algunos ambientes puede ser muy frecuente).
- Debe establecer la política de reutilización, a fin de que las contraseñas no puedan ser reutilizadas al menos en un año.
- Deberá establecer que las contraseñas tengan *al menos* una extensión de ocho caracteres. En las contraseñas en las que no importa que se escriban en mayúsculas o minúsculas y que no permiten caracteres especiales, esto nos da un total de 368 permutaciones posibles, o casi 3 billones de posibilidades. Si el NOS utiliza contraseñas en las que sí importa que se escriban en mayúsculas o minúsculas, las posibilidades son todavía mayores: 628 (218 billones), respectivamente. En sistemas que permitan que los caracteres especiales sean parte de la contraseña (caracteres como el espacio, la coma, el punto, el asterisco, etc.), el número de combinaciones posibles es aún mayor. Incluso 2 mil millones de posibilidades es mucho: si alguien fuera capaz de probar una contraseña por segundo, tendría que pasar 63 años probando con todas las permutaciones. O bien, con un programa optimizado que pudiera probar 5 millones de posibilidades en un segundo, le tomaría aproximadamente un año descifrar una contraseña de ocho caracteres en mayúsculas o minúsculas mezcladas utilizando la fuerza bruta.



PISTA Muchos programas descifradores de contraseñas dependen de diccionarios de palabras y nombres comunes a fin de reducir de manera significativa el número de posibilidades que tengan que probar. Debido a esto, recomiéndeles a los usuarios crear contraseñas que no sean palabras en cualquier idioma o, si son palabras, que tengan números y otras caracteres no alfanuméricos insertados en algún lugar en la palabra, a fin de que un "ataque con diccionario" no dé resultado. Asimismo, invite a los usuarios a usar contraseñas con mayúsculas y minúsculas mezcladas en redes que las soporten.

- Asegúrese de poner en marcha cualquier política que supervise y se ocupe de la gente que ingresa contraseñas incorrectas. A menudo llamadas *detectores de intrusos*, estas políticas detectan cuando alguien ha intentado varias veces ingresar a la red con contraseñas incorrectas. Si ocurren varios intentos en un periodo determinado, el sistema bloquea la cuenta del usuario, previendo así que se hagan más intentos. Me gusta establecer esta característica, de manera que bloquee una cuenta cada vez que se ingresen cinco contraseñas incorrectas en una hora y, después, bloquear la cuenta hasta que sea reestablecida por el administrador. De esta forma, si alguien ingresa un gran número de contraseñas incorrectas, tendrá que hablar con el administrador para reabrir la cuenta, y usted podrá saber por qué se dio esta situación y corregirla. En general, el usuario olvida su contraseña y trata de ingresar con varias incorrectas; sin embargo, alguien pudiera estar tratando de adivinarla, por lo que amerita que se analice esta situación (preguntándole al usuario si los intentos fueron de él) a fin de eliminar la última posibilidad.
- NetWare de Novell y Windows Server le permiten establecer límites sobre cuándo y dónde un usuario puede firmarse en la red. Usted puede delimitar el tiempo durante el día en el que se le permite al usuario firmarse y también puede restringir el acceso de una cuenta a determinadas computadoras de la red. Hacer lo anterior para todos los usuarios de la red no es justificable; sin embargo, usted querrá considerar restringir la cuenta administrativa a varias estaciones de trabajo, de forma que alguna persona en una estación de trabajo diferente (o que acceda a la red a través de una conexión WAN), no pueda ingresar a la cuenta, aun si esa persona conoce la contraseña.

PISTA Considere la posibilidad de llevar a cabo auditorias periódicas a las contraseñas, a fin de que compruebe la seguridad de sus contraseñas de red utilizando herramientas comercialmente disponibles diseñadas para obtener las de los usuarios. (Estas herramientas no funcionan sin la contraseña del administrador y, a menudo, requieren acceder físicamente al servidor). Los programas para auditar pueden adivinar las contraseñas de su red utilizando una gran cantidad de métodos y generarán un reporte donde se especifique cuánto tiempo les llevó adivinarlo. Las contraseñas verdaderamente seguras no se pueden adivinar en un tiempo razonable. De manera sorprendente, cuando usted realiza una auditoria por primera vez, le sorprenderá descubrir que muchas de las contraseñas que se utilizan en la red no son seguras y se adivinan en cuestión de segundos. Le recomiendo un gran programa para las redes basadas en Windows llamado LC4 de una compañía llamada @Stake (**http://www.atsstake.com**). Usted puede utilizar lo que aprenda de un programa como LC4 con el objetivo de diseñar sus propias políticas sobre las contraseñas para que sean más seguras.

Existe un *catch-22* muy interesante que se relaciona con las políticas de seguridad de una red: Si las hace *muy* estrictas, en realidad *reduce* la seguridad de su red. Por ejemplo, suponga que establece que se acceda a la red con contraseñas de 12 caracteres, que forzosamente se tengan

¿Existen alternativas para las contraseñas?

Hay un gran número de alternativas para crear contraseñas, las cuales hacen las redes más seguras y la seguridad de éstas más simple para los usuarios. La primera alternativa es algo que se llama *identificación del factor-2*, que es un sistema por medio del cual el usuario lleva a todos lados una pequeña faltriquera electrónica del tamaño de un conector USB, la cual despliega un conjunto de números que cambia constantemente y que son específicos a ésta. El usuario recuerda solo un número de identificación personal (NIP) de cuatro dígitos. Cuando los usuarios se firman en la red, ingresan el número que está programado en ese momento en la faltriquera más su NIP. Debido a que el sistema de la red cuenta con un inventario de faltriqueras para comparar, sus secuencias de números y también tiene el NIP del usuario, éste puede identificarse de forma bastante segura. Si se pierde una faltriquera, puede desactivarse de manera muy sencilla en el sistema y se generará una nueva. La identificación del factor 2 a menudo se utiliza para identificarse en el acceso remoto.

Otra alternativa que ha surgido, y cuyo uso se está generalizando, es utilizar información biométrica, como los lectores de huellas dactilares. Para cuando se escribió este libro, éstos no se encontraban disponibles para su uso corporativo; no obstante, usted podrá observar que estos equipos se están moviendo con celeridad en esta dirección. Microsoft ahora ofrece dispositivos (como el teclado con un lector integrado) que puede explorar las huellas dactilares de los usuarios e ingresarlas a un sistema. Existen otras compañías que venden dispositivos similares. Sin embargo, al menos en el caso de los dispositivos de Microsoft, las empresas fabricantes establecen que no se hicieron para fines corporativos. Creo que no está lejos el día en que las computadoras vengan equipadas con lectores de este tipo y que los usuarios solamente tengan que colocar su dedo en el lector a fin de identificarse en el sistema de manera segura.

que cambiar una vez a la semana y que no se permita la reutilización de contraseñas. La mayoría de los usuarios no podrá recordar de una semana a otra qué contraseñas están usando y, como es natural, acabarán escribiendo su contraseña en algún lugar de su oficina. Por supuesto, una contraseña escrita es mucho menos segura que una guardada en la mente. El truco de la seguridad de la red estriba en el equilibrio entre la seguridad y la facilidad de uso.

Permisos de archivo y directorio

El segundo tipo de seguridad interna que usted necesita para conservar la información de su red implica el acceso del usuario a archivos y directorios. Estos parámetros son, en realidad, un poco más difíciles de administrar que las cuentas de usuario, ya que por lo general tiene al menos 20 directorios y muchos cientos de archivos por cada usuario que tenga en la red. El gran volumen de directorios y archivos hace que la administración de estos parámetros sea una tarea difícil. No obstante, la solución es establecer procedimientos regulares, seguirlos y, después, auditar partes del árbol de directorios, en particular áreas que contengan archivos sensibles, de manera periódica. Asimismo, estructure todos los directorios de la red con el fin de que pueda, en la mayoría de las áreas, asignar permisos en los niveles superiores, los que "fluirán hacia abajo" automáticamente a los subdirectorios, lo cual hace mucho más fácil revisar quién tiene acceso a qué directorios.

Los NOS tienen una flexibilidad considerable en cuanto a los permisos que le permiten establecer en los archivos y directorios. Utilizando los permisos incluidos en el NOS, puede habilitar a los usuarios en diferentes roles en cualquier directorio. Estos roles controlan qué pueden hacer y qué no los usuarios dentro de ese directorio. Como ejemplos de roles genéricos de directorio se incluyen los siguientes:

- **Crear solamente** Este tipo de rol permite a los usuarios agregar un archivo nuevo a un directorio, sin embargo, los restringe de ver, editar o eliminar los archivos existentes, incluyendo cualquiera que ellos hayan creado. Este tipo de rol es perfecto para permitir a una persona agregar nueva información a un directorio al que, de otra forma, no debería tener acceso. El directorio se vuelve casi un buzón de correo en la esquina de una calle. Usted solamente puede poner cosas nuevas en él. Por supuesto, otro usuario tendrá acceso total al directorio y podrá sacar y trabajar con los archivos.
- **Solo lectura** Este rol permite que los usuarios vean los archivos de un directorio y los jalen a fin de que los puedan ver en su computadora. Sin embargo, los usuarios no pueden editar o cambiar los archivos almacenados de ninguna forma. Este tipo de rol es bueno para desplegar material publicado a los usuarios que necesiten ver la información, pero que no puedan modificarla. (Los usuarios con privilegios de lectura pueden copiar un archivo de un directorio de solo lectura a otro directorio y, después, hacer lo que quieran con ella. Dichos usuarios no podrán cambiar la copia almacenada en el directorio de solo lectura).
- **Modificar** Este rol permite a los usuarios hacer lo que deseen con los archivos de un directorio, excepto que no pueden proporcionar a otros usuarios el acceso a éste.
- **Control total** Este rol, generalmente reservado para el “propietario” de un directorio, permite que el (los) propietario(s) haga lo que quiera con los archivos de un directorio y, además, le permite otorgar a otros usuario el acceso a él.

Los roles están creados de formas distintas en los diferentes NOS. El capítulo 17 proporciona más detalles acerca de cómo los sistemas operativos Windows Server manejan los permisos de directorio.

Así como usted puede otorgar permisos para acceder a los directorios, también puede otorgar seguridad a archivos específicos. Los permisos de archivos funcionan de manera similar a los permisos de directorios. En el caso de archivos específicos, puede controlar que un usuario lea, modifique o elimine un archivo. Los permisos de archivos generalmente anulan los permisos de directorio. Por ejemplo, si ciertos usuarios hubieran cambiado el acceso a un directorio, pero usted limita su permiso para acceder a un archivo en ese directorio a solo lectura, esos usuarios solamente tendrían acceso de solo lectura a ese archivo.



PISTA Para una red de cualquier tamaño, recomiendo evitar el uso de permisos de red a archivos específicos, excepto en muy raros casos. La razón es que podría hacerse un verdadero relajo recordar a qué archivos tiene permiso especial cada usuario de acceder o a qué archivos hay que proporcionar permiso de acceso a un empleado nuevo.

Prácticas y educación del usuario

El tercer tipo importante de seguridad interna tiene que ver con la parte más insegura de cualquier red: la gente. Usted debe preocuparse de dos cosas: primero, necesita establecer prácticas

y hábitos para tener una buena seguridad. No es suficiente diseñar e implantar un gran esquema de seguridad si no lo administra bien todos los días. Para establecer buenas prácticas, necesita documentar procedimientos relacionados con la seguridad y, después, implantar algún tipo de proceso a fin de asegurarse que los empleados sigan los procedimientos en forma regular. De hecho, usted estará mucho mejor si cuenta con un simple diseño de seguridad que se siga al pie de la letra, que con un diseño de seguridad excelente pero complejo y que no sea acatado. Por esta razón, mantenga el diseño general de seguridad de la red tan simple como le sea posible, siempre y cuando éste se mantenga coherente con las necesidades de la compañía.

Usted también necesita asegurarse —tanto como le sea posible— de que los usuarios siguen los procedimientos prudentes, algunos de los cuales se pueden cumplir fácilmente por medio de los parámetros del NOS; sin embargo, debe manejar otros por medio del entrenamiento. Algunos consejos para facilitar esto son los siguientes:

- Infórmele a los usuarios qué se espera de ellos en términos de seguridad. Proporcióneles un documento que describa la seguridad de la red y las acciones que necesitan hacer para preservarla. Dentro de los lineamientos que deberán seguir los usuarios se encuentran la selección de contraseñas seguras, no proporcionar sus contraseñas a nadie, no dejar sus computadoras abandonadas por periodos prolongados mientras están firmados en la red, no instalar software que no sea de la compañía, entre otras acciones.
- Cuando ingresen a la compañía nuevos empleados y sean capacitados acerca del uso de la red, asegúrese de explicar los problemas de seguridad.
- Dependiendo de la cultura de la compañía, haga que los usuarios firmen un documento, en el que reconozcan que conocen los procedimientos principales acerca de la seguridad que la empresa espera que sigan.
- De manera periódica, audite las acciones de seguridad de los usuarios. Si tienen acceso total a los directorios, examine cómo asignaron permisos a los demás usuarios.
- Asegúrese de revisar los registros de seguridad del NOS que utilice. Investigue y dé seguimiento a cualquier problema que se reporte.



PISTA Es una buena idea documentar cualquier problema que encuentre relacionado con la seguridad. Mientras que la mayoría son benignos, en ocasiones puede encontrar alguno en el que el usuario haya fallado en su intento. En dichos casos, su registro acerca de lo que encontró y las acciones que tomó pueden ser muy importantes.

Mientras que es importante planear para el peor caso cuando se diseña y administra la seguridad de una red, es necesario también darse cuenta de que la mayoría de las veces los problemas relacionados con la seguridad surgen de la ignorancia u otras causas inocentes y no de algún intento malicioso.

COMPRENDER LAS AMENAZAS EXTERNAS

La *seguridad externa* es el proceso de asegurar la red contra amenazas externas. Antes de Internet, este proceso no era difícil. La mayoría de las redes tenía módems externos solamente para que los usuarios marcaran a la red y era sencillo mantener seguros esos puntos de acceso. Sin embargo,

con el surgimiento de Internet y el hecho de que casi todas las redes se conectan a ella, la seguridad se ha convertido en algo mucho más importante y también más complejo.

Al inicio de este capítulo, usted leyó que jamás está totalmente segura una red. Esto es válido cuando se trata de la seguridad externa de una red conectada a Internet. Casi todos los días, los hackers descubren nuevas técnicas para romper la seguridad de una red a través de una conexión a Internet. Aun si encontrara un libro que estudiara todas las amenazas a un tipo especial de red, el libro estaría obsoleto al poco tiempo de su impresión.

Existen tres tipos básicos de amenazas contra la seguridad externa:

- **Amenazas por la puerta de enfrente** Estas amenazas surgen cuando una persona ajena a la compañía encuentra, adivina o viola una contraseña de usuario y luego entra a la red. El perpetrador puede ser alguien que tuvo relación con la compañía en algún momento o alguien que no tiene relación alguna con ésta.
- **Amenazas por la puerta de atrás** Estas son amenazas donde los defectos en el software o el hardware del sistema operativo de la red facilitan a una persona ajena a la compañía violar la seguridad de la red. Después de lograr lo anterior, con frecuencia esta persona encuentra una forma de tener acceso a la cuenta del administrador y hacer lo que se le antoje. Las amenazas por la puerta de atrás también pueden programarse deliberadamente en el software que usted utiliza.
- **Negación del servicio** Estos son ataques que niegan el servicio de la red. Entre los ejemplos se encuentran cometer acciones específicas que se sabe que dejan fuera de servicio a los diferentes tipos de servidores o que inundan la conexión a Internet de la compañía con basura (como una inundación de solicitudes ping).



NOTA Existe un cuarto tipo de amenaza externa: los virus de la computadora, los caballos de Troya, los gusanos y otro software malicioso proveniente de un punto fuera de la compañía. Estas amenazas se estudian en una sección dedicada a ellas dentro de este capítulo.

Por fortuna, usted puede hacer una gran cantidad de cosas a fin de implantar medidas robustas relacionadas con la seguridad externa. Probablemente éstas no alejen a un intruso determinado y muy habilidoso; sin embargo, dichas medidas pueden hacer su trabajo tan difícil que hagan que se rinda y se vaya a otro lugar.

Amenazas por la puerta de enfrente

Las *amenazas por la puerta de enfrente*, en las que alguna persona fuera de la compañía puede acceder a una cuenta de usuario, son con seguridad las amenazas de las que es necesario que usted se proteja mejor. Estas amenazas pueden tomar muchas formas. La más común es el empleado descontento o que fue despedido de la empresa y que alguna vez tuvo acceso a la red. Otro ejemplo es alguien que trata de investigar o adivinar la contraseña de una cuenta válida en la red, o que, de alguna forma, obtiene una contraseña válida del propietario de ésta.

El personal dentro de la compañía, ya sea actual o exempleado, es potencialmente el más peligrosos de todos. Dicho personal tiene muchas ventajas que un intruso no tiene. Conoce los nombres de usuario importantes que ya están en la red, por lo que sabe sobre qué cuentas ir. Es probable que conozca las contraseñas de usuario desde el tiempo en que estuvo trabajando para la compañía. Asimismo, conoce la estructura de la compañía, cuáles son los nombres de los servidores y otra información que hace más fácil violar la seguridad de la red.

La protección contra una amenaza por la puerta de enfrente rodea a una robusta protección contra la seguridad interna, ya que, la seguridad externa e interna se encuentran íntimamente relacionadas. Este es el tipo de amenazas donde todas las políticas y prácticas estudiadas en la sección acerca de la seguridad interna pueden ser de gran ayuda a fin de prevenir problemas. Usted también puede tomar medidas adicionales con el objeto de protegerse contra amenazas por la puerta de enfrente:

- Mantenga los recursos de la red que deban accederse desde la LAN separados de los recursos que deban accesarse desde fuera, siempre que sea posible. Aquí está un ejemplo: quizá tenga la suerte suficiente de nunca proporcionar a los usuarios externos acceso al servidor del departamento de contabilidad de la empresa. Usted puede hacer casi imposible acceder a ese sistema desde fuera de la LAN, por medio de una serie de medidas. Puede instalar el ruteador del firewall para eliminar cualquier acceso a través de éste hacia las direcciones IP o IPX del servidor. Si el servidor no requiere una IP, puede eliminar ese protocolo. Además, puede configurar el servidor para negar el acceso fuera de las horas normales de trabajo. Dependiendo del NOS que corra en el servidor, podrá restringir el acceso a las direcciones MAC de Ethernet a las máquinas de la LAN que deban acceder al servidor. También puede configurar el servidor para permitir que cada usuario entre al servidor solo una vez. Los pasos específicos que puede tomar dependen del servidor en cuestión y del NOS que esté corriendo, sin embargo, el principio básico sigue siendo válido: separe los recursos internos de los externos siempre que sea posible.
- Lleve un control de qué usuarios pueden acceder a la LAN desde otro punto fuera de ésta. Por ejemplo, puede correr un software VPN para sus usuarios viajeros o con oficina en casa para acceder a la LAN de manera remota vía Internet. Así, debe habilitar este acceso solo a usuarios que lo necesiten y no a todos los que probablemente lo necesiten.
- Considere la configuración de las cuentas de acceso remoto para los usuarios remotos de forma independiente de sus cuentas normales y restrínjalas más que sus cuentas normales de la LAN. Es probable que esto no sea práctico en muchos casos, sin embargo, es una estrategia que puede ayudar, en particular, a usuarios que tienen una amplia seguridad para acceder a la LAN.
- Para los módems a los que los usuarios marcan desde un punto fijo, como desde sus casas, configure sus cuentas para que utilicen *marcación de regreso*. Ésta es una característica por medio de la cual usted marca de manera segura el número telefónico del sistema desde el que los usuarios están llamando (por ejemplo, desde sus números telefónicos en casa). Cuando los usuarios deseen conectarse, marcan el teléfono del sistema, solicitan acceso y, después, el sistema de acceso remoto termina la conexión y marca el número telefónico preprogramado para hacer la conexión real. Su computadora contesta la llamada y, después, procede a conectarlos normalmente. Alguien que trate de acceder al sistema desde otro número telefónico no podrá entrar si usted tiene habilitada la función de marcación de regreso.
- Si un empleado con acceso libre sale de la compañía, revise las cuentas de usuario de éste de las que se pueda saber la contraseña. Planee un cambio obligado de contraseñas a dichas cuentas una vez que el empleado se haya ido.



NOTA Un aspecto importante de la seguridad tanto interna como externa es la seguridad física. Asegúrese de que el cuarto en el que se encuentran sus servidores esté cerrado y sea un lugar seguro.

Las personas que traten de acceder a la red que no están asociados con la compañía, en un momento determinado, pueden tratar de usar una técnica llamada, de manera optimista, *ingeniería social*, que consiste en que utilizan métodos no técnicos para conocer las cuentas de los usuarios y las contraseñas dentro de la compañía. Estas técnicas son más peligrosas en grandes compañías, donde no todos los empleados se conocen entre sí. Un ejemplo de una técnica de ingeniería social es llamar a un empleado y fingir que es un administrador de red, que está rastreando un problema y necesita la contraseña del empleado en ese momento. Otro ejemplo es escudriñar en la basura de la compañía a fin de encontrar los registros que puedan ayudarlo a hallar una contraseña. Asegúrese de instruir a los empleados de la compañía para que nunca proporcionen su contraseña por teléfono a ninguna persona y que no es necesario que alguna persona de buena fe del departamento de tecnología de la información de la compañía les pregunte su contraseña.

Amenazas por la puerta de atrás

Las amenazas por la puerta de atrás a menudo se refieren a problemas con el NOS en sí o a algún otro punto de la infraestructura de la red, como los ruteadores. No cometa ningún error, todos los NOS y la mayoría de los componentes de la red tienen agujeros de seguridad. Lo mejor que usted puede hacer para evitar estos problemas es actualizar su software del NOS y cualquier parche relacionado con seguridad que sea liberado. También deberá revisar periódicamente nueva información acerca de agujeros de seguridad que se descubran en el software del NOS que utilice (¡y no confíe en el sitio web del fabricante para encontrar la mejor información acerca de esto!). Un buen sitio web que puede usar para mantenerse actualizado en cuanto a agujeros de seguridad es el que mantiene el Computer Emergency Response Team (CERT), ubicado en **http://www.cert.org**. Además de encontrar consejos sobre agujeros de seguridad, puede encontrar información de seguridad muy valiosa en este sitio.

Los servidores web son un objetivo frecuente para los intrusos. Tome en cuenta los consejos siguientes para protegerse contra las amenazas a los servidores de la web:

- Usted estará más seguro si puede almacenar el sitio web de la compañía en un servidor externo (como un sistema de ISP) en lugar de en su propia red. No solamente un ISP es más capaz para proporcionar servicio al servidor las 24 horas del día, siete días a la semana, sino que probablemente también sea más seguro. Además, no es necesario que se preocupe porque un servidor web acceda a su LAN desde fuera de la compañía, lo cual, a veces, deja abiertos otros agujeros.
- Asegúrese de implantar un ruteador robusto de firewall en su red. Los ruteadores de pared se analizan con mayor profundidad en el capítulo 3. No obstante, debe tener a una persona que conozca su firewall y su servidor de web para que efectúe pruebas a su configuración o le ayude con ella. Recuerde, los firewall también necesitan tener actualizado su software.

¡DEFÍNALO! Zona desmilitarizada

Cuando usted pone computadoras entre su firewall (en el otro lado de la firewall respecto a su red) y su conexión hacia una red externa, como Internet, al área entre esos dos dispositivos se le llama *zona desmilitarizada*, o DMZ para abreviar. En general, una organización colocará su servidor público de red en la DMZ, y esa computadora no tendrá ningún tipo de información confidencial. De esta manera, si la seguridad de esa computadora es violada, el intruso no tendrá acceso a la red en sí.

- Asegúrese de que ha revisado con cuidado los parámetros apropiados de seguridad de su servidor web, que los ha implantado todos y de manera ocasional efectúenles auditorias.
- Considere la colocación de un servidor web, diseñado por personal ajeno a su compañía, fuera de su pared (en otras palabras, entre la firewall y el ruteador que lo conecta a Internet —a esta área se le conoce como “zona desmilitarizada”—). De esta forma, aun si alguien es capaz de irrumpir en el servidor de la web, le costará mucho trabajo acceder al resto de la red.
- Salvaguarde su tráfico de correo electrónico. El correo electrónico es una de las formas más comunes de traer virus o programas caballo de Troya a su compañía. Asegúrese de correr software explorador de virus apropiado para su servidor de correo electrónico y que las firmas de los virus se actualicen *todos los días*.

Amenazas de negación del servicio

Los ataques de *negación del servicio (DoS)* son aquellos que niegan el servicio de un recurso de la red a usuarios legítimos. A menudo, están enfocados a los servidores de correo electrónico y servidores de web, sin embargo, pueden afectar a la red entera. Los ataques DoS, en general, se presentan en una de dos formas: pueden negar el servicio inundando la red con tráfico basura, o pueden aprovecharse de los errores en el software de la red para acceder a los servidores. Los ataques DoS contra un servidor de correo electrónico generalmente inundan el servidor con correo hasta que éste niega el servicio a usuarios legítimos o se satura debido a la intensa carga de información.

Para prevenir ataques DoS, asegúrese de mantener actualizados los diferentes tipos de software de red. Asimismo, utilice los parámetros en su firewall para deshabilitar el servicio de tráfico Internet Control Message Protocolo (ICMP) (que maneja las solicitudes ping) de la red y niegue el acceso a los servidores fuera de la LAN que no necesiten tener accesos desde fuera de la LAN. Por ejemplo, el servidor del sistema de contabilidad de la compañía. En dicha situación, usted podría configurar la firewall o el ruteador de filtrado de paquetes a fin de negar todo el tráfico foráneo hacia y desde la dirección IP de ese servidor.

VIRUS Y OTRO SOFTWARE MALICIOSO

Desafortunadamente, una cantidad cada vez mayor de software malicioso se encuentra circulando alrededor del mundo. Existen muchos tipos de software diferentes, incluyendo los siguientes:

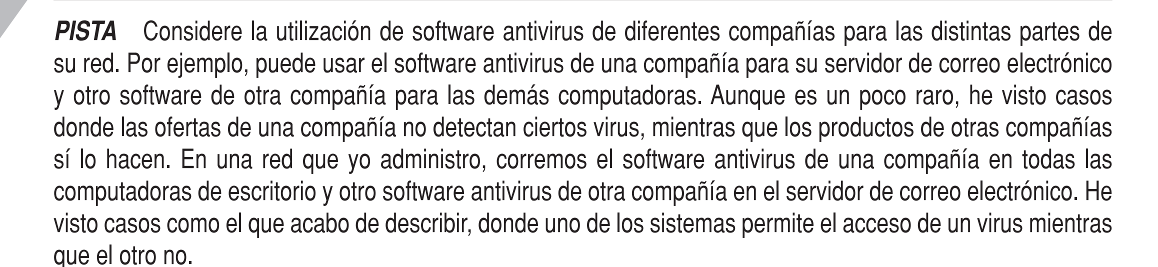
- **Virus** Un *virus* de computadora es un programa que se disemina infectando a otros archivos con una copia de ellos mismos. Entre los archivos que pueden infectarse por virus están los de programa (COM, EXE y DLL) y de documentos de aplicaciones que soportan macrolenguajes tan complicados para permitir el comportamiento del virus. (Word y Excel de Microsoft son objetivos muy comunes de los virus basados en macros). A veces aun los archivos de datos como los de imagen JPG pueden ser infectados por sofisticados virus.
- **Gusanos** Un *gusano* es un programa que se propaga enviando copias de sí mismo a otras computadoras, que corren el gusano, que a su vez envían copias a otras computadoras. En años recientes, los gusanos se han difundido a través de sistemas de correo electrónico junto con un mensaje que invita al receptor a abrir los archivos adjuntos que contienen el gusano, el cual envía copias de sí mismo a otra gente definida en el libro de direcciones del correo electrónico del usuario, sin que éste sepa que esto está sucediendo. Lo mismo ocurre con la gente que recibe los correos. Un gusano como este puede difundirse en cuestión de horas a través de Internet.
- **Caballos de Troya** Un *caballo de Troya* es un programa que tiene como objetivo hacer algo interesante o útil y que después lleva a cabo acciones maliciosas tras bambalinas mientras que el usuario está interactuando con el programa principal.
- **Bombas lógicas** Las *bombas lógicas* son porciones maliciosas de código de programación insertadas en un programa normal. A menudo, el autor original del programa o alguien más que participe en el desarrollo del código fuente, las inserta. Las bombas lógicas pueden programarse para ejecutarse en cierto tiempo, borrando los archivos clave o llevando a cabo otras acciones.

En la actualidad existen más de 70 000 virus conocidos y diariamente se descubren más. Estos virus representan una gran amenaza para cualquier red y un aspecto importante de la administración de su red es protegerla de ellos.

Para proteger una red de los ataques de virus, usted necesita implantar algún tipo de software antivirus, que corre en computadoras de la red y "busca" virus conocidos o alguna actividad parecida a la de éstos. De este modo, el software elimina el virus, dejando el archivo original intacto, lo pone en cuarentena a fin de que pueda ser verificado por el administrador o bloquea el acceso al archivo de alguna otra forma.

El software antivirus funciona en la mayoría de las computadoras de la red, como servidores de archivos, de impresión, de correo electrónico, computadoras de escritorio y hasta en firewalls computarizadas. Además, se encuentra disponible en un gran número de fabricantes, entre los tres más importantes Symantec (Norton Antivirus), TrendMicro (PC-cillin) y Network Associates (McAffe VirusScan). Su mejor apuesta es asegurarse de que se corra el software antivirus en todos sus servidores y que se configure de forma que se actualice con frecuencia (cada varios días, o mejor todavía, todos los días). (Usted puede configurar la mayoría del software antivirus mediante el servidor a fin de actualizar, de manera automática,

su lista de virus conocidos a través de una conexión de Internet). Asimismo, debido a que el correo electrónico es el mecanismo principal de transmisión de virus por computadora en estos días, asegúrese de correr software antivirus en su servidor de correo electrónico y, si es posible, recomiendo que se actualicen las firmas de los virus en el servidor de correo electrónico cada hora. Lo anterior es debido a que los nuevos virus transportados por correo electrónico pueden difundirse por todo el mundo muy rápido, en cuestión de horas. Si actualiza de manera automática su software antivirus de su correo electrónico cada hora, es más probable que logre la actualización antes de que los virus afecten su red.



PISTA Considere la utilización de software antivirus de diferentes compañías para las distintas partes de su red. Por ejemplo, puede usar el software antivirus de una compañía para su servidor de correo electrónico y otro software de otra compañía para las demás computadoras. Aunque es un poco raro, he visto casos donde las ofertas de una compañía no detectan ciertos virus, mientras que los productos de otras compañías sí lo hacen. En una red que yo administro, corremos el software antivirus de una compañía en todas las computadoras de escritorio y otro software antivirus de otra compañía en el servidor de correo electrónico. He visto casos como el que acabo de describir, donde uno de los sistemas permite el acceso de un virus mientras que el otro no.

Usted también deberá corre el software antivirus en sus estaciones de trabajo, sin embargo, no deberá confiar en ese software como su recurso principal para eliminar virus. En lugar de depender de dicho software como su protección principal, considere el software antivirus de escritorio como un complemento de su software basado en el servidor.

RESUMEN DEL CAPÍTULO

Aun si se dedicara todo un libro al tema de la seguridad de las redes, no podría aprender todo lo que se necesita para proporcionar a una red toda la seguridad posible. Constantemente se descubren nuevas amenazas y el cambiante panorama del software hace que dicha información se haga obsoleta de manera muy rápida. En lugar de eso, en este capítulo aprendió acerca de amenazas de seguridad comunes y recibió consejos que le pueden ayudar a formular e implantar buenas prácticas de seguridad. En especial, debe tener a un consultor de seguridad externo a fin de que le ayude a diseñar sus planes de seguridad y a revisarlos y auditarlos de forma regular.

Por último, si usted es responsable de la seguridad de la red, debe saber que es un trabajo que nunca termina y del que nunca conoce lo suficiente. Necesita invertir tiempo para aprender más acerca de las particularidades del tema de la seguridad, en especial de los NOS que usted utiliza en su red. Los libros siguientes pueden ayudarle a mejorar su educación acerca de la seguridad de las redes:

- Maiwald, Eric, *Network Security: A Beginner´s Guide*, segunda edición, McGraw-Hill/Osborne, 2003.
- McClure, Stuart, Joel Scambray y George Kurtz, *Hacking Exposed: Network Security Secrets and Solutions*, quinta edición, McGraw-Hill/Osborne, 2005.

- Hare, Chris, y Karanjit Sayan, *Internet Firewalls and Network Security*, segunda edición, New Riders Publishing, 1996. (Es un libro viejo pero tiene una explicación excelente de la verdadera "seguridad", es decir, a niveles del Departamento de Defensa. El libro también describe cómo desarrollar políticas de seguridad de la red en una compañía y explica el filtrado de paquetes y la tecnología de pared).
- Meinel, Carolyn P., *The Happy Hacker: A Guide to (Mostly) Harmless Computer Hacking*, cuarta edición, American Eagle Publishing, 2002. Es una excelente introducción a la actividad del intruso. El libro aplica un método de "cómo hacer" y enseña tanto al principiante como el personal con experiencia encargado de la seguridad de las redes qué buscar todos los días.

CAPÍTULO 12

Restablecimiento de los desastres de la red

Los servidores de red contienen recursos vitales de la compañía, en forma de información, conocimiento y trabajo invertido de los empleados. La mayoría de las empresas, si fueran de repente despojadas para siempre de estos recursos, no podrían continuar sus negocios de manera ininterrumpida y tendrían que encarar pérdidas de millones de dólares, tanto por pérdida de información como por las consecuencias que esto traería. Por tanto, tener un plan para el restablecimiento de desastres en las redes, formular e implantar la estrategia de respaldo de la red son dos de las tareas más importantes en la administración de las redes.

Este capítulo analiza estos dos temas. Usted aprenderá acerca de los problemas que debe resolver en un plan de restablecimiento de desastres y también sobre los sistemas y las estrategias para respaldar la red. Sin embargo, antes de abordarlos, debe leer acerca de las experiencias del restablecimiento de desastres que ocurrieron en la ciudad de Seattle.

NOTAS DESDE EL LUGAR DE LOS HECHOS: LA CIUDAD DE SEATTLE

El editor técnico de la primera a la tercera edición de este libro, Tony Ryan, tuvo una experiencia personal con el restablecimiento de los desastres de la red. Tony trabajaba en el Departamento de Tecnología de la Información de la ciudad de Seattle. El 28 de febrero de 2001, la ciudad experimentó un terremoto que provocó que se pusieran a prueba los planes de restablecimiento de desastres de la ciudad. Lo que sigue a continuación son los comentarios de Tony respecto a las operaciones de restablecimiento de desastres y cómo la ciudad manejó los problemas que ocurrieron en la agitación del terremoto. Este es un excelente ejemplo de por qué necesita contar con una planeación contra desastres y saber cómo ésta debe abarcar todos lo eventos posibles.

Notas del terremoto de 2001 en Seattle y su restablecimiento del desastre

por Tony Ryan

Seattle ha experimentado algunos hechos muy inusuales que atrajeron la atención en los últimos años. Entre éstos vale la pena mencionar la conferencia de la Organización Mundial de Comercio (WTO) en 1999 y las demostraciones violentas que la acompañaron, las cuales fueron transmitidas a todo el mundo por televisión e Internet. Asimismo, se presentaron motines durante las celebraciones del Mardi Gras en el 2000. Sin embargo, nada es comparable con el daño potencial causado por el terremoto de 6.8 grados que azotó a la ciudad el miércoles 28 de febrero de 2001.

La situación del EOC

La ciudad de Seattle cuenta con un Centro de Operaciones de Emergencia (OEC, por sus siglas en inglés) que se activa durante cualquier evento o crisis que tenga un impacto potencial en la seguridad pública, o que, de otra forma, afecte a cualquier número de servicios ofrecidos por la ciudad o sus habitantes.

A veces, el EOC puede activarse antes de tiempo, por ejemplo, en el Y2K y en el aniversario de las demostraciones de la WTO. Revisar los preparativos que se llevaron a cabo para esos eventos y compararlos con lo que pasó durante los sucesos no planeados como el terremoto, ayuda a ilustrar algunos principios importantes acerca del restablecimiento de desastres del área de Tecnología de la Información y de cómo estar preparado para ellos.

Nunca suponga

Durante los preparativos del Y2K, se les pidió a los miembros de mi grupo que aumentaran el personal que normalmente se asigna para dar soporte a las PC de escritorio, laptops e impresoras del EOC. El equipo que soporta el EOC pertenece a una organización de TI diferente a la nuestra, y como puede esperarse, su forma de hacer las cosas difiere de la nuestra por muchas razones válidas. Sin embargo, una vez que mi grupo tuvo la oportunidad de observar el ambiente de la EOC, pudo compartir algunas nuevas perspectivas y métodos que fueron bienvenidos y adoptados por el grupo de soporte de la EOC y todo el personal involucrado tuvo una idea de cuál podría esperase que fuera la forma "estándar" de configurar las PC de la EOC. Los ejemplos varían desde codificación compleja de ciertos modelos de NIC de PC para que trabajen mejor en los switches dentro de su closet de cableado, hasta desarrollar e implantar una imagen base para todas las laptops que se utilizarían en el edificio. Como resultado, el Y2K fue reconocido como un ejemplo de la cooperación entre grupos del área de tecnología de la información y de la excelente preparación en general. ¡Fue una mañana de sábado muy tranquila!

¿Cambio de administración?

Sin embargo, entre estos sucesos hubo una gran cantidad de tiempo y oportunidades para que las cosas cambiaran. La instalación pudo haberse utilizado para otros propósitos de negocios; el equipo (como las laptops) pudo haberse prestado, o los clientes pudieron hacer uso del equipo; y otros grupos de tecnología de la información, además del nuestro, pudieron ayudar al grupo y realizar modificaciones en las configuraciones que no se documentaron o no se comunicaron a todos los involucrados.

Los resultados

Lo que haya sucedido sigue siendo un misterio. Lo que en realidad descubrimos después del terremoto fue que cuando clientes que normalmente utilizan el EOC en situaciones de emergencia quisieron usar el equipo, en algunos casos las máquinas no trabajaron como se esperaba: el software no podía cargarse en una PC, la laptop ya no se conectaba a la red, algunas PC no eran las mismas o se les había cambiado el procesador por unos menos potentes. Las cosas habían cambiado y el resultado fue que parte del trabajo de emergencia que los profesionales en tecnología de la información, como los técnicos en soporte a la web, tuvieron que llevar a cabo, tomó más tiempo del que habíamos previsto. De manera irónica, la web desempeñó un papel crucial en nuestra "estrategia" general de comunicaciones. El impacto del equipo de cómputo que no estaba trabajando de manera adecuada no fue evidente todavía; sin embargo, los eventos siguientes ilustran cómo pudieron haber sucedido.

Unos minutos después del azote del terremoto, algunos edificios del centro en los que los empleados de la ciudad de Seattle trabajaban, fueron evacuados debido al miedo a daños estructurales. Aunque nadie resultó herido y, de manera sorprendente, solo dos teclados se rompieron de todos los edificios a los que les proporcionamos ayuda, imagínese a un par de miles de personas muy asustadas y preocupadas corriendo por las banquetas y en las calles, saturando las redes telefónicas celulares en desesperados intentos por contactar a sus seres queridos y buscando cualquier forma posible de comunicación —en especial a gerentes como yo y otros grupos de supervisión, quienes poseemos varios niveles de entrenamiento contra desastres.

Afortunadamente, el alcalde de la ciudad había enviado representantes a los puntos de reunión indicados donde el staff debería concentrarse en caso de estos eventos, quienes informaron a las personas que estaban en los edificios principales afectados que regresaran a casa. Con ese aviso, el CTO nos pidió a todos que "verificáramos la web" para buscar información; lo cual significaba revisar el sitio web interno de la ciudad. Sin embargo, ¿qué pasaría si la PC del EOC hubiera sido cambiada (digamos) por una Pentium 133 con 64 MB de RAM y que, por tanto, no pudiera correr el programa FrontPage 2000 de Microsoft? Si ese sitio web tuviera que ser actualizado con noticias e información oficial de manera rutinaria, los resultados hubieran podido ser confusos e inconvenientes.

Contingencia y costos

Debido a que somos una entidad consolidada y de carácter público, somos muy cuidadosos acerca de cómo gastamos el dinero de nuestros clientes, puesto que la empresa está sujeta a una supervisión muy estricta (y es correcto que así sea). A menudo, los clientes no poseen los fondos para gastarlos en equipo moderno para PC que corra la última versión de Windows y una PC de repuesto para colocarla en el closet nada más "por si acaso". Después del terremoto, un par de edificios quedaron inutilizables temporalmente hasta que los inspectores examinaran los daños a fin de ver si eran seguros para los empleados. En realidad, uno de ellos alberga a una gran cantidad de personal de nuestro staff de tecnología de la información y, como resultado, no solamente tuvimos que buscar "PC de repuesto" para que las usaran nuestros clientes (mientras buscaban otras oficinas), sino que nosotros, como soporte del grupo de tecnologías de la información nos vimos en la necesidad de hacer lo mismo. El efecto inmediato: en pocas ocasiones tuvimos dificultades para apoyar a nuestros clientes tan pronto como nuestros contratos sobre el nivel de servicio lo establecían, en particular debido a que no pudimos reingresar inmediatamente a nuestro edificio donde teníamos nuestras PC y otro equipo necesario.

Lección aprendida: tenga respuestas a la mano... al menos algunas

Así, parece que tarde o temprano se paga… Tiene sentido mantener un porcentaje de PC disponible para esos eventos especiales; podría servir de 10 a 15% del inventario de repuesto. Tome en cuenta que los negocios de cualquier giro están obligados en dichas situaciones a llevar a cabo un tipo de "compromiso" en el que determinen cuáles funciones de su negocio son más críticas y cuáles pueden posponerse —hasta que su existencia completa de equipo pueda reconectarse o reemplazarse— por lo que se justifica ese 10 a 15%.

Diseñe un plan de comunicaciones y la forma como se comunicará

Volvamos al anuncio del CTO. Algunos se preguntaron: "¿Qué hay de los que no tienen acceso a la web en casa?". Como grupo de tecnología de la información, inquirimos: "¿Qué pasará si los servidores web han sido destruidos en su totalidad?". (De hecho, algunos desechos del techo del cuarto en el que se encontraban los servidores cayeron cerca de ellos, pero no sufrieron dañados y el servicio nunca se interrumpió). Otros se cuestionaron: "¿Qué sucede con quienes no escucharon el mensaje y no saben que tienen que entrar a la web?". Estas situaciones y "qué hacer en caso de…" pueden resolverse con la ayuda de un plan de comunicaciones claro y siempre a la mano. Irónicamente, dichos planes se habían llevado a cabo a detalle en otros eventos; sin embargo, en el caso de una "emergencia" real, nosotros, como departamento, no habíamos identificado un plan a seguir. Una prioridad de nuestro departamento es reexaminar esa situación y diseñar una estrategia, utilizando las comunicaciones que se desarrollaron para el Y2K y casos por el estilo como modelos.

Otro punto: como se mencionó anteriormente, nuestro staff no es responsable de dar soporte al EOC de manera rutinaria. A pesar de que estamos muy dispuestos a cooperar en ese soporte, como lo evidencia el que lo hayamos hechos en algunas ocasiones. Casi inmediatamente después del terremoto, recibí un mensaje solicitándome que enviara técnicos al EOC para que proporcionaran soporte a los funcionarios de la ciudad que se reportaban en ese lugar durante emergencias. Aunque nuestro equipo no tenía ningún acuerdo con el EOC para proporcionar soporte aun "por solicitud", inmediatamente pedí a dos de mis técnicos, que habían trabajado en el EOC anteriormente, que respondieran, y se reportaron ahí y dieron soporte al edificio hasta que el staff asignado llegó. Nunca se puso en duda que teníamos que acudir cuando se nos solicitara; sin embargo, pregunté a nuestro director divisional si era apropiado desarrollar de manera más clara las expectativas, o incluso un acuerdo SLA, entre nuestro staff y el EOC, y él estuvo conforme. No investigué si el personal en el EOC tiene permiso por ley de utilizar "todos" los recursos de la ciudad en caso de una emergencia, pero un acuerdo claro podía permitirme designar a una persona de mi staff que actuara de manera proactiva y llamara al EOC en esas circunstancias.

Debo aclarar que ninguno de estos preparativos puede sustituir a la gente inteligente y dedicada. El ejemplo más brillante es el de uno de mis técnicos que proporciona soporte a los programadores responsables de la aplicación de la nómina en la ciudad. Esta persona tuvo la disposición para llegar a trabajar temprano el día después del terremoto y, de alguna forma, persuadió al grupo de construcción y a los inspectores de que le permitieran el acceso al edificio. Subió 13 tramos de escalera, recogió una PC y sus periféricos, la bajó y la llevó a otro edificio y la configuró para trabajar en un segmento en el nuevo edificio de forma que el programador pudiera efectuar las operaciones necesarias para que se hiciera la nómina de la ciudad ese fin de semana y los empleados pudieran recibir su pago a tiempo, como se esperaba. Más que esto no se puede pedir.

PLANES DE RESTABLECIMIENTO EN CASO DE DESASTRES

Un plan de restablecimiento en caso de desastres es un documento que analiza cómo se recupera una red de un desastre que ponga en peligro su información o que haga que deje de funcionar. A menudo, los auditores financieros externos de una compañía requieren planes anuales de restablecimiento en caso de desastres, debido a la importancia que tiene para el negocio la información y al efecto que dicha falla en la red pudiera tener en la compañía. Además, los planes de restablecimiento en caso de desastres también son importantes ya que obligan al administrador de la red a pensar en todos los escenarios posibles. Al considerar todos estos escenarios, el administrador podrá hacer planes más eficientes a fin de proteger la información de la red contra pérdidas y restablecer las operaciones del negocio tan pronto como sea posible. Como se mencionó en la introducción de este capítulo, la planeación del restablecimiento en caso de desastres y la administración de los sistemas de respaldo de la compañía son las dos tareas más importantes del administrador de la red.

La mayoría de las compañías no tienen planes de restablecimiento de desastres demasiado grandes. Para una red de varios cientos de nodos y 15 o más servidores, dicho plan generalmente consiste de 10 a 20 páginas aproximadamente o menos, aunque su extensión varía en función de la complejidad de las operaciones que se lleven a cabo en la red de la compañía. (Las 500 compañías de la revista *Fortune*, por ejemplo, pueden tener planes de restablecimiento de desastres de más de cien páginas, tomando en cuenta todos sus sitios). Una estrategia para mantener los planes de restablecimiento de desastre concisos y maximizar su utilidad es enfocarse en problemas que, aunque sea remota su ocurrencia, de alguna forma tienen probabilidad de suceder. De manera alternativa, puede enfocarse en los resultados del desastre: qué pasa, en vez de tratar de encontrar las causas del desastre: por qué pasó. (Enfocar su plan en los resultados del desastre significa tomar en cuenta cosas como la pérdida de un solo servidor, de todo el cuarto del servidor, de todas las computadoras tipo estación de trabajo utilizadas para dar servicio al cliente, etc., sin preocuparse de qué posibles desastres pudieron causar esos resultados).

Las secciones siguientes analizan los problemas clave mínimos que un plan de restablecimiento debe considerar. En función de su propia compañía, su plan podrá tomar en cuenta problemas adicionales.

Análisis de necesidades

Antes de elaborar un borrador del plan real, usted debe analizar qué necesidades deberá satisfacer dicho plan, las cuales podrán variar en función de quién requiera entrar al proceso de planeación de restablecimiento de desastres y qué problemas quiera esta gente que el plan incluya. Considere estos tipos de necesidades:

- Planear de forma organizada las contingencias y asegurarse de que se han considerado todos los desastres posibles y se han definido las contramedidas del plan.
- Asegurar a los auditores de contabilidad externos de la compañía que ésta ha considerado y desarrollado planes para manejar desastres.
- Informar a la alta dirección de la compañía acerca de los riesgos que existen en la red y sus datos en diferentes situaciones, y en cuánto tiempo se espera resolver cualquier problema que se pudiera presentar.

- Solicitar a la alta dirección de la compañía que establezca prioridades en cuanto al restablecimiento y al mínimo de requerimientos aceptables para restablecer servicios.
- Planear formalmente con las áreas clave del negocio de su compañía (por ejemplo, manufactura, servicio a clientes, ventas), las consideraciones alrededor de los tipos de desastres relacionados con las computadoras o problemas serios.
- Asegurarse de que los clientes de la compañía están tranquilos acerca de que las operaciones de datos de ésta se encuentran seguras contra cualquier tipo de desastre.

Sólo una vez que haya identificado las necesidades que el plan deba satisfacer, usted podrá comenzar con el proceso de planeación con una visión clara de qué deberá contemplar el plan. Asimismo, sabrá a quiénes de las diferentes partes de la compañía deberá involucrar en el proceso de planeación.

Escenarios de desastres

Usted debe comenzar el proceso de planeación considerando diferentes escenarios de desastre posibles. Por ejemplo:

- Un incendio en el cuarto del servidor —en cualquier otra parte del edificio— destruye las computadoras y las cintas.
- Una inundación que afecte el cuarto del servidor destruye alguna computadora o batería de respaldo que se encuentra tan cerca del piso como para ser afectada. (Recuerde que las inundaciones bien pueden ser provocadas por algo que se encuentra dentro del mismo edificio, como una fuga de agua en el cuarto contiguo o la presencia de fuego que active los aspersores de agua).
- Un problema eléctrico que provoca la falla de las fuentes de alimentación.
- Algún problema que ocasiona la pérdida total de conectividad hacia el exterior. Por ejemplo, un enlace WAN crítico o un enlace a Internet pueden interrumpirse por alguna razón.
- Una falla estructural de algún tipo en el edificio que afecte la red y los servidores.
- Alguno de los problemas anteriores afecta a computadoras críticas para las operaciones de la empresa en cualquier lugar del edificio. Por ejemplo, el problema puede suceder en las áreas de manufactura, en el centro de servicio a clientes o, quizás, en el closet o cuarto donde se encuentre el sistema telefónico.

Aunque ninguno de estos eventos es muy probable que ocurra, es importante considerarlos. El punto principal de la planeación del restablecimiento en caso de desastres es prevenir o minimizar pérdidas serias, y el proceso es de muy poca utilidad si solo considera aquellos desastres que piensa que son los más probables de que sucedan.

Después de considerar desastres como los que se acaban de mencionar, debe tomar en cuenta las fallas graves que pudieran afectar las operaciones de la red. Aquí se presentan algunos ejemplos de éstas:

- La tarjeta madre en su servidor principal falla y el proveedor no puede conseguir el reemplazo en menos de tres días.
- Los discos de uno de sus servidores fallan de forma que se pierden los datos. Si usted está corriendo algún tipo de esquema de disco redundante (RAID), realice planes que consideren fallas que sean más críticas que las del sistema RAID pueda proteger. Por ejemplo, si utiliza controladores RAID 1 en espejo, haga planes que tomen en cuenta la falla en ambos lados del espejo en el mismo lapso. Si está utilizando RAID 5, podría considerar que se presente una falla en cualquier par de controladores al mismo tiempo.



NOTA Los arreglos de discos RAID se estudian a detalle en el capítulo 13.

- Su controlador de respaldo de cinta falla y no puede repararse antes de una o dos semanas. Aunque esto no provoca una pérdida de datos en sí misma, ciertamente aumenta la probabilidad de quedar expuesto a este problema.

Usted debe planear cómo respondería a éstas y otras posibles fallas. Si la tarjeta madre de su servidor principal falla, querrá hacer planes para cambiar de forma temporal sus controladores a otra computadora compatible. Si su disco falla, debe diseñar un plan en el cual usted puede reconstruir el arreglo de discos y recuperar la información lo más pronto posible a partir de sus respaldos. Si su controlador de respaldo de cinta falla, es probable que quiera saber qué tan rápido podría conseguir un controlador equivalente o si el fabricante del controlador de cinta podría proporcionarle controladores de reemplazo reacondicionados en poco tiempo a cambio de su controlador que está fallando. Para todas esas fallas, querrá considerar el costo de contar con refacciones o con servidores completos de respaldo, de forma que pueda restablecer sus operaciones lo más rápido posible. Usted deberá considerar e investigar todos los tipos de respuesta posibles que se enuncian a continuación:

- ¿Deberá tener un contrato de mantenimiento? (Si es así, asegúrese de que comprende a detalle sus garantías y procedimientos).
- ¿Deberá tener en existencia ciertas partes para que se encuentren disponibles en caso de una falla?
- ¿Existen otras computadoras disponibles que puedan utilizarse como reemplazo de un servidor clave mientras éste se repara? ¿Qué sucede con los componentes que no sean de cómputo, pero que sean importantes, como ruteadores, hubs o switches?
- Si usted necesita tomar medidas temporales, ¿están entrenados los empleados afectados para hacer su trabajo con el reemplazo que les proporcione o sin el sistema si fuera necesario? Por ejemplo, si los sistemas electrónicos de un restaurante no estuvieran funcionando, ¿podría el restaurante (y los servidores, el equipo de la cocina, los cajeros, etc.) operar el negocio en forma manual hasta que se repare el sistema?
- ¿Deberá mantener un sito de restablecimiento frío o caliente? Un sitio de restablecimiento "frío" es un cuarto que su propia compañía mantiene y que está cerca del centro de datos protegidos. El sitio frío tiene energía eléctrica, aire acondicionado y otras instalaciones necesarias para albergar al sitio en caso de que el centro de datos experimentara algún desastre. Un cuarto "caliente" es lo mismo que uno frío, excepto que además cuenta con

el equipo de cómputo y software necesarios para duplicar las funciones de procesamiento del centro de datos. Las compañías que llevan a cabo operaciones muy delicadas y críticas con datos, a menudo mantienen sitios de restablecimiento frío o caliente.

El proceso de considerar posibles problemas, como desastres o fallas de piezas de equipo clave y, después, hacer planes para controlarlos es, con certeza, la esencia de la planeación del restablecimiento de desastres. Sin embargo, su plan escrito deberá también analizar o resolver otros problemas, los cuales se estudian en las secciones siguientes.

Comunicación

Una parte importante de cualquier plan de restablecimiento de desastres tiene que ver con la forma como manejará las comunicaciones. Sin una comunicación efectiva, sus intentos para manejar el desastre serán en vano, y la demás gente no podrá realizar su trabajo tan bien como debiera.

Comience haciendo una lista de las diferentes instancias que podrían necesitar ser notificadas de un problema, su avance hacia su solución y su resolución final. Su lista deberá verse como lo siguiente:

- El consejo de administración
- El presidente o director general
- Los vicepresidentes de área
- El vicepresidente o gerente del área afectada
- Su supervisor
- Empleados afectados por el problema

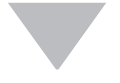
Para cada una de estas instancias —cualquier otra que pueda identificar— necesita considerar qué nivel de problema requiere su notificación. El consejo de administración, por ejemplo, es muy probable que no necesite saber acerca de un desastre a menos que sea probable que tenga un efecto material en el desempeño de la compañía. Por otro lado, es posible que su supervisor quiera ser notificado acerca de todo problema que se presente y, seguramente, cualquier empleado afectado necesita también ser notificado.

Una vez que haya listado las instancias por notificar y los aspectos sobre los que es necesario informarles, deberá considerar *cómo* se los informará. Si usted es la persona a cargo de la resolución del desastre, es mejor delegar la notificación a alguien más que no esté tan involucrado de manera directa, a fin de que pueda enfocarse en resolver el problema tan pronto como sea posible. Por ejemplo, la tarea de comunicarle a la gente adecuada debe ser delegada a su supervisor o a algún empleado que trabaje en el mismo departamento que usted y que esté libre de manejar esta tarea. Quien sea que sea deberá contar con todos los procedimientos de comunicación y, él o ella, deberá tener acceso a toda la información necesaria de los contactos: los números telefónicos de casa, los números de beeper, de teléfonos celulares, etc., para las situaciones que requieran de ser notificadas fuera del horario de trabajo. Es probable que también desee configurar una árbol de teléfonos a fin de notificar de manera más rápida. Por último, de acuerdo con su ambiente y con los diferentes tipos de desastres, usted necesitará especificar el orden en el que se le notificará al personal, el cual no necesariamente es igual al orden que sigue la estructura organizacional de la compañía.

El plan de restablecimiento de desastres escrito deberá incluir toda la información anterior.

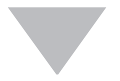
ALMACENAMIENTO FUERA DEL SITIO

El almacenamiento fuera del sitio es una forma importante de protección de sus cintas de respaldo en el caso de que un desastre físico, como un incendio, destruya todas sus copias. Debido a que el almacenamiento fuera del sitio es un aspecto muy importante de la protección contra desastres, debe ser incluida en su plan de restablecimiento.



NOTA Si usted no tiene todavía un procedimiento de almacenaje fuera del sitio, debe considerar muy en serio adoptar uno. Aunque los archiveros a prueba de fuego puedan proteger sus cintas contra incendios moderados, no son invulnerables a incendios muy intensos o prolongados. Además, las cintas son más sensibles al humo y al calor que los papeles que un archivero a prueba de fuego pueden proteger.

Las compañías que ofrecen almacenamiento de archivos fuera del sitio a menudo proporcionan prácticas estandarizadas para el almacenamiento de cintas. Estas compañías trabajan con base en la rotación, en la que un chofer de la compañía de almacenamiento acude a sus oficinas periódicamente —generalmente una vez por semana— y entrega un grupo de cintas al mismo tiempo que recoge otro. Estas compañías por lo general utilizan cajas de acero inoxidable para transportar las cintas, y el administrador de la red es el responsable de mantener las cajas bajo llave y de guardar las llaves. Usted necesita decidir qué cintas se deberán quedar en el sitio y cuáles enviar fuera de él. Una regla general es conservar siempre los dos respaldos más recientes en el sitio (a fin de que estén disponibles para restablecer los archivos eliminados por los usuarios) y enviar las cintas más antiguas fuera de éste. De esta forma, usted tiene a la mano las cintas que necesita de manera regular, a la vez que minimiza su riesgo a que sean afectadas por desastres. Después de todo, si un desastre destruye el cuarto del servidor y todas las cintas que estén dentro, probablemente no estará tan preocupado de haber perdido la información de una semana solamente.



NOTA La cantidad de datos que puede exponer a un desastre varía considerablemente en función de la naturaleza del negocio de su compañía y de los datos. Algunas operaciones son tan sensibles que la pérdida de datos de tan solo algunos minutos sería catastrófica. Por ejemplo, un banco simplemente no puede perder ni una sola transacción no importando lo que pase. Los negocios que necesitan proteger información extremadamente sensible a menudo contratan a un proveedor para que les proporcione almacenamiento de datos en línea fuera del sitio. Dicho proveedor replica la información del negocio en los servidores del fabricante a través de una conexión de alta velocidad, como una T-1 o T-3. Es usual que estos proveedores también ofrezcan servicios de atención a fallas, en los que sus computadoras pueden llevar a cabo los trabajos en caso de una avería. De manera alternativa, si un negocio opera en varios sitios, el proveedor puede configurar el software y los procedimientos que le permitan ofrecer los mismos servicios utilizando sus propios sitios.

Componentes críticos de la reconstrucción

Su plan deberá describir qué equipo de cómputo y software se requerirá a fin de restablecer las operaciones en caso de que el edificio resulte en una pérdida total. Esta lista deberá estimar a groso modo el costo del equipo y cómo se puede obtener pronto. Al preparar dicha lista, puede reducir el tiempo que se requiere para continuar con las operaciones de manera temporal en un edificio. Asimismo, si su compañía adquiere un seguro contra interrupciones en las operaciones de su negocio, necesitará dichos estimados para la póliza de seguros.

RESPALDO Y RESTABLECIMIENTO DE LA RED

Un plan de restablecimiento en caso de desastres de la red no tiene ningún valor si no cuenta con alguna forma para restablecer los datos almacenados en el servidor. Aquí es donde entran el respaldo y el restablecimiento de la red. Si usted es un administrador, o tiene aspiraciones de llegar a serlo, entonces ya debe saber acerca de la importancia de hacer buenos respaldos en el sistema y de la información importante. Si todavía no lo sabe, entonces es probable que la lección más importante que pueda aprender de este libro sea: hacer respaldos regularmente es un requisito cuando se utilizan computadoras, punto.

Usted no requiere gran experiencia del trabajo con las computadoras antes de que se dé cuenta de la importancia de realizar buenos respaldos. Las computadoras pueden fallar y fallan, y a veces yerran en formas que hacen irrecuperable la información almacenada en ellas. O, quizás, eventos extraños provocan que se eliminen o sean corrompidos algunos archivos importantes. En casos como éstos, los trabajos se recuperan o pierden con base en la calidad de los respaldos que se hagan y la habilidad de restablecer la información importante.

Evaluación de las necesidades

Antes de diseñar los procedimientos de respaldo de una red, primero tiene que evaluar las necesidades de la compañía. En particular, necesita comprender muy bien las necesidades de respaldo de la compañía. Preguntas como las que a continuación se listan le podrán ayudar a comprender las necesidades que debe satisfacer:

- ¿Qué tan dinámico es el almacenamiento de datos en los servidores? ¿Con qué frecuencia se modifica y de qué manera lo hace?
- ¿Qué cantidad de datos necesita respaldarse y a qué velocidad crecen éstos?
- ¿Cuánto tiempo se tiene disponible para realizar el respaldo? Asegúrese de evitar situaciones donde necesite respaldar terabytes de datos utilizando un sistema que solo puede manejar megabytes por hora.
- Si se requiere un restablecimiento parcial o completo de un respaldo, ¿qué tan rápido se debe hacer éste? Como regla general, el restablecimiento de datos toma cerca del doble de tiempo que su respaldo; aunque en algunos casos, los tiempos pueden ser aproximadamente los mismos. En otras palabras, si a su sistema de respaldo le toma 10 horas en la noche respaldar toda la red, le tomará de 10 a 20 horas restablecer los datos; y este lapso no incluye el tiempo que se requiere para resolver cualquier problema necesario para restablecer datos en primer lugar.
- ¿Qué tan coherente necesita ser el respaldo de datos? En otras palabras, ¿una colección de archivos de datos necesita ser manejada como una sola unidad? Por ejemplo, un directorio que contenga muchos archivos generados en un procesador de palabra no es muy coherente, así que puede restablecer uno, muchos o todos sin preocuparse de cómo afectarán a los demás archivos. Por otro lado, una colección de archivos de base de datos de una base grande, a menudo, no es de mucha utilidad a menos que pueda restablecer *todos* los archivos de la colección, y a partir *exactamente* del mismo instante. (Las bases de datos grandes —como las de Oracle— que requieren este tipo de respaldo seguramente contarán con instrucciones propias explicadas a detalle sobre cómo deberá realizarse dicho respaldo).

- ¿Qué relación debe haber entre el costo y la capacidad de recuperación? Usted puede diseñar sistemas de respaldo que operen minuto a minuto a fin de que si algo falla, el sistema no pierda datos, y que la administración pueda tener un alto grado de confianza en esto. (Por ejemplo, un banco requiere de este tipo de sistema de respaldo). Sin embargo, estos sistemas de respaldo cuestan mucho dinero y requieren de mucha administración. La mayoría de las compañías con gusto negociarían ese costo tan elevado por un menor grado de recuperación, como tener respaldos nocturnos del sistema. ¿Qué necesita su compañía y cuánto está dispuesta a pagar?
- ¿Cuántos niveles de redundancia necesita la compañía para sus respaldos? La mayoría de los respaldos se hacen en cintas y servidores de soporte que utilizan arreglos RAID, por lo que las cintas son, en realidad, el *segundo* nivel de protección. En algunos casos, puede requerirse múltiples cintas, cada una con una copia por separado del respaldo. Otra forma de obtener redundancia máxima es proporcionar una copia de los respaldos a una compañía de almacenamiento de datos por medio de algún tipo de conexión de red.

Cuando realice su evaluación, es importante involucrar a la alta dirección de su compañía en el proceso. Como mínimo, usted deberá presentarle sus opciones y obtener su visto bueno, así como sus comentarios.

Adquisición de tecnologías y medios de respaldo

Una vez que usted tenga alguna idea de sus necesidades de respaldo, puede proceder a adquirir el software y hardware necesarios para crear y administrar sus respaldos.

Suponiendo que necesite comprar hardware nuevo para el respaldo de un sistema, existen un gran número de opciones comprobadas dependiendo de sus necesidades reales. Cuando seleccione una tecnología de respaldo, considere los factores siguientes:

- Confiabilidad del hardware y del medio.
- Costo del hardware y del medio.
- Capacidad de almacenamiento.
- Frecuencia probable de las recuperaciones.
- La importancia de colocar la totalidad del respaldo en un solo equipo de hardware.

La tabla 12-1 repasa tipos diferentes de tecnologías de respaldo, su costo aproximado y las ventajas y desventajas relativas. Observe que los precios de los controladores, el medio y los costos por megabyte que se estipulan en la tabla 12-1 son aproximados.

Si su compañía puede comprar cintas DLT y puede hacer uso de sus capacidades (también se encuentran disponibles controladores DLT más pequeños), usted deberá considerar definitivamente comprar esta tecnología. Las cintas DLT son muy robustas, pueden utilizarse un millón de veces y se dice que tienen una vida de 30 años. Además, los controladores son muy rápidos tanto para respaldos como para recuperaciones. Incluso, existen robots autocambiadores disponibles para los controladores DLT, lo que significa que existe mucho espacio para las cabezas por si usted sobrepasa el límite del tamaño del controlador con el que cuente. Además, los sistemas de robots son relativamente baratos y existe una amplia variedad de ellos: desde sistemas pequeños que pueden dar cabida a cinco cintas solamente, hasta grandes bibliotecas que pueden albergar a decenas o cientos de ellas.

Nombre	Costo aproximado del controlador*	Costo aproximado del equipo*	Capacidad del equipo	Ventajas y desventajas
Controladores ZIP	150 (0.75–1.50/MB)	15 each (0.075–0.15/MB)	1–750MB	+ Acceso remoto – Muy baja capacidad – Baja velocidad
Controladores JAZ	500 (0.50/MB)	100 (0.10/MB)	1GB	+ Acceso remoto – Baja capacidad – Baja velocidad
Controladores CD-R/RW	200 (0.32/MB)	1–5 (0.002–0.008/MB)	650MB	+ Acceso remoto – Baja capacidad – Baja velocidad – El medio CD-ROM no es reutilizable
Controladores DVD-ROM/RW	500 (0.083/MB)	10 (0.001/MB)	4–8GB	+ Acceso remoto + Gran capacidad – Baja velocidad
Controladores QIC-80/Travan	250–500 (0.03–0.05/MB)	30 (0.003/MB)	5–40GB	+ Costo del controlador muy bajo/MB – Más lento que otras cintas
Controladores DAT DDS-1	500 (0.167/MB)	20 (0.007/MB)	2–4GB	– El más caro/MB que el QIC/Travan – Baja capacidad de cinta
Controladores DAT DDS-2	800 (0.10/MB)	25 (0.003/MB)	8GB	+ Costo más bajo/MB que el DDS-1 o el QIC/Travan
Cinta de 8mm	1 500 (0.188/MB)	50 (0.006/MB)	8GB	+ Tecnología probada – Ya no es competitiva en cuanto a costo respecto a las capacidades actuales de los DAT/QIC – Tiempos de búsqueda de la cinta para la recuperación de archivos individuales relativamente bajos

(* en dólares)

Tabla 12-1. Tipos de tecnologías de respaldo.

Nombre	Costo aproximado del controlador*	Costo aproximado del equipo*	Capacidad del equipo	Ventajas y desventajas
Enorme (8mm)	4 000 (0.026/MB)	90 (0.0006/MB)	150GB	+ Tecnología probada + Cinta de alta densidad + Rápida – No tiene un uso muy extenso (comparada con DLT)
Cinta lineal digital (DLT)	3 000 (0.038/MB)	<50 (0.0005/MB)	80GB	+ Muy confiable + Muy rápida + Altas capacidades por cinta + Costo del equipo extremadamente bajo/MB
Super cinta lineal digital (SDLT)	5 000 (0.016/MB)	80 (0.00025/MB)	320GB	+ Muy confiable + Muy rápida + Altas capacidades por cinta + Costo del equipo extremadamente bajo/MB
Cinta lineal abierta (LTO)	5 000 (0.013/MB)	80 (0.00020/MB)	400GB	+ Muy confiable + Muy rápida + Altas capacidades por cinta + Costo del equipo extremadamente bajo/MB – Nuevo formato de cinta

(* en dólares)

Tabla 12-1. Tipos de tecnologías de respaldo (continuación).

Algunas de las tecnologías de respaldo más novedosas, como la SuperDLT 320 (320GB por cinta) y LTO 3 (400 GB por cinta), prometen mejorar las DTL anteriores. Para redes muy grandes, estas tecnologías que están surgiendo pueden tener sentido y su uso se diseminará en los próximos años.

Selección de las estrategias de respaldo

Después de conseguir toda la información necesaria, usted puede planear una estrategia de rotación del respaldo de su información, la cual contemplará la forma como se llevará a cabo. La rotación de respaldo está diseñada para cumplir con los objetivos siguientes:

- En caso de una falla catastrófica, reconstruya el sistema con los datos más recientes posibles.
- Recupere los archivos de las cintas más antiguas que tal vez hayan sido borradas o dañadas por accidente sin que alguna persona se haya dado cuenta de la pérdida potencial de los datos.
- Protéjase contra fallas en el sistema de respaldo.
- Proteja sus datos de una posible falla provocada por el ambiente, como un incendio que destruya el sistema original y los datos.

La mayoría de los sistemas operativos de red reservan bits especiales para cada archivo del sistema. Uno de estos se conoce como *bit de archivo*, el cual indica el estado de respaldo del archivo. Cuando un usuario modifica un archivo, su bit de archivo queda fijo en "encendido", indicando que el archivo debe estar respaldado. Una vez que se finaliza el respaldo, el bit de archivo se apaga. Al utilizar este bit de archivo y su software de respaldo, usted puede realizar los tipos de respaldo siguientes:

- Un *respaldo completo*, donde todos los directorios y archivos seleccionados son respaldados, sin considerar el estado de su bit de archivo. Los respaldos completos ponen en cero el bit de archivo de todos los archivos respaldados cuando éstos finalizan.
- Un *respaldo incremental*, donde solamente se respalda los archivos que tenga el bit de archivo. Lo anterior respalda todos los archivos modificados desde el último respaldo total o incremental. Los respaldos incrementales ponen en cero el bit de archivo de los archivos respaldados, los cuales no se respaldarán durante el siguiente respaldo incremental a menos que se modifiquen otra vez y sus bits de archivo sean cambiados al estado "encendido".
- Un *respaldo diferencial*, el cual es similar al incremental en el sentido de que respalda solamente los archivos que tengan su bit de archivo activo. La diferencia fundamental en un respaldo diferencial es que los bits de archivo se dejan activos. Los respaldos diferenciales subsecuentes respaldarán los mismos archivos de nuevo, además de cualquier otro que haya sido modificado.

En un mundo perfecto, sería maravilloso realizar siempre respaldos completos; de manera que si el sistema llegara a fallar, entonces solo necesitaría las cintas de respaldo más recientes para recuperar el sistema en su totalidad. Sin embargo, por un gran número de razones, llevar a cabo un respaldo completo a menudo no es factible. Es posible que no haya tiempo suficiente para llevar a cabo un respaldo completo todos los días. Otra razón es extender la vida del equipo y del controlador de cinta, reduciendo la cantidad de trabajo que llevan a cabo. Sin embargo, necesita ponderar estas cuestiones contra el tiempo que toma la recuperación a partir de una combinación de respaldos total, incremental o diferencial, y la posibilidad mayor de no poder recuperar los respaldos adecuadamente utilizando una combinación de los métodos. (Por ejemplo, si una recuperación total requiriera un respaldo total de la semana anterior, además de cuatro respaldos incrementales desde entonces, usted cuenta con las cinco cintas en estado perfecto y estaría expuesto a la posibilidad de que una cinta no estuviera en buen estado).

Una forma común de mezclar estos tipos de respaldos es realizar un respaldo completo del sistema una vez por semana y llevar a cabo respaldos incrementales y diferenciales todos los días. Analice los ejemplos siguientes:

- Usted hace un respaldo completo todos los viernes por la noche y respaldos incrementales de lunes a jueves. Si el sistema falla el lunes por la mañana, antes de que ingrese al sistema algún dato, necesita recuperar solamente el respaldo completo a partir de la noche del viernes anterior. Sin embargo, si el sistema falla en la mañana del jueves, por ejemplo, usted tendrá que respaldar cuatro cintas en forma secuencial a fin de recuperar toda la información; el respaldo completo del viernes anterior, y después las cintas incrementales del lunes, martes y miércoles por la noche. Además, para garantizar la integridad de los datos, debe ser capaz de recuperar todas esas cintas y hacerlo en su secuencia apropiada. De otra forma, corre el riesgo de acabar con los archivos de datos que no coincidan. En este escenario, tiene cuatro puntos de falla basados en el medio de almacenamiento, lo cual podría provocar más riesgo del que puede tomar.
- Usted hace un respaldo completo todos los viernes por la noche y respaldos diferenciales de lunes a jueves de cada semana. En este escenario, si el sistema falla el lunes por la mañana, solamente recupera la cinta de la noche del viernes anterior. Sin embargo, si el sistema falla el jueves por la mañana, usted tendrá que recuperar dos cintas solamente: el último respaldo completo de la noche del viernes, además del respaldo diferencial del miércoles por la noche. Debido a que los respaldos diferenciales respaldan todos los archivos que sufrieron alguna modificación desde el último respaldo completo, usted nunca necesitará recuperar más de dos cintas, reduciendo de esta forma el número de posibles puntos de falla del equipo.

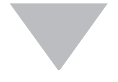
La regla general es: los respaldos incrementales generalmente minimizan la cantidad de tiempo necesaria para llevar a cabo cada respaldo diario, sin embargo, toman más tiempo para recuperarse y representan un mayor riesgo de falla del equipo. Los respaldos diferenciales toman más tiempo, pero reducen el tiempo requerido para recuperar la información y también el riesgo de una falla en el equipo.

Así que para determinar el mejor esquema de respaldo para su sistema, usted necesita balancear la naturaleza de los datos y la cantidad de riesgo que esté dispuesto a tomar contra el costo de cada respaldo, la capacidad de las cintas y la cantidad de tiempo que tome hacer cada respaldo regular.

El esquema más común de rotación de respaldos se llama Abuelo-Padre-Hijo (GFS). Una forma muy común de implantarlo es utilizar al menos ocho cintas. Le coloca etiquetas a cuatro cintas que vayan de "lunes" a "jueves" y marca las otras cuatro como "viernes 1", "viernes 2" a "viernes 4". Cada lunes a jueves, utiliza una de las cintas correspondientes, reemplazando la información almacenada la semana anterior. Cada cinta viernes corresponde a un viernes del mes a partir del primer viernes, de manera que empieza con la de viernes 1, y así sucesivamente. Por último, el último día del mes, prepara una cinta de fin de mes, la cual no vuelve a utilizar y la mantiene fuera del sitio en caso de que una falla en el ambiente destruya el sistema y todas las cintas almacenadas localmente.

Existen tres variaciones principales del esquema GFS. En la primera, usted solo hace un respaldo completo del sistema cada vez que lleve a cabo un respaldo. Esta variación proporciona la mayor cantidad de redundancia y el menor tiempo de recuperación.

En la segunda, usted realiza un respaldo completo de cada una de las cintas de los viernes y de la cinta mensual, sin embargo, hace solamente respaldos incrementales durante la semana. En la tercera, usted hace algo muy parecido a lo anterior, pero utilizando respaldos diferenciales en lugar de incrementales.



PISTA Si sus datos son extremadamente críticos y no reconstruibles con facilidad, puede llevar a cabo respaldos completos todas las noches y también un respaldo incremental rápido a la hora de la comida. De esta forma, solo perderá mediodía de información.

También puede seleccionar esquemas de rotación más simples que el GFS. Por ejemplo, puede utilizar dos o tres cintas y después rotarlas en secuencia, sobreescribiendo en los datos antiguos cada vez. Lo anterior permite recuperar cualquier información de los tres días anteriores. La desventaja de este esquema es que, a veces, será necesario que vaya hacia atrás en el tiempo a fin de poder recuperar los datos que habían sido borrados o dañados sin que nadie se diera cuenta inmediatamente. Usted puede atacar este problema utilizando varias cintas, las cuales rotará de manera semanal o mensual.

Un factor que se debe tener en mente cuando se consideren diferentes esquemas de rotación de las cintas es la *granularidad* de sus respaldos. En general, la granularidad se refiere a la flexibilidad que tiene para recuperar datos de cintas anteriores. En el esquema GFS estándar, donde se hacen respaldos completos todo el tiempo, puede recuperar un archivo a partir de cualquier día de la semana, de cualquier fin de semana (viernes) dentro del mes o de cualquier mes durante el año. Sin embargo, no puede recuperar un archivo que fue creado tres meses atrás a la mitad del mes y fue borrado o (dañado) antes de que terminara el mes, ya que no existirá una copia limpia en cualquiera de la cintas de respaldo. El mejor consejo para seleccionar el esquema de rotación de información importante es: a menos de que existan razones para hacerlo de otra forma (como

Granularidad y corrupción de datos: un balance truculento

Una razón por la que hay que considerar la granularidad con mucho cuidado es la posibilidad de que los datos se destruyan sin que se pueda notar. Por ejemplo, trabajé una vez con un archivo de base de datos que se había afectado varias semanas antes, pero que seguía trabajando de manera normal y parecía que estaba en buen estado. Sin embargo, después de que se empezaron a presentar problemas, el equipo de soporte técnico del fabricante de la base de datos encontró que una parte de ésta, que no se utilizaba con regularidad, se había perdido y que era imposible recuperarla. El problema fue provocado por un sector defectuoso en el disco duro de la base de datos. La única forma en la que el personal de soporte podía recuperar la base de datos y asegurarse de que estuviera limpia fue recuperar los respaldos yendo hacia atrás en el tiempo, hasta que encontraran una copia de la base de datos que no hubiera sido dañada. Entonces, volvieron a ingresar los datos que habían sido agregados desde el momento en que se hizo la copia no dañada. Debido al amplio margen de tiempo entre respaldos, a medida que el personal de soporte escarbó más y más, la cantidad de datos que necesitamos realimentar creció casi de manera exponencial.

ya se analizó), utilice el esquema GFS con respaldos completos todas las veces. Lo anterior maximiza la seguridad de su información y la flexibilidad de recuperación, y minimiza el riesgo de una falla en el equipo. Si los demás factores lo obligan a seleccionar un esquema diferente, utilice el análisis que se realizó en este capítulo a fin de que pueda llegar a la mejor decisión de su situación particular.

RESUMEN DEL CAPÍTULO

Usted puede ser la persona más versada en el mundo de la conectividad de redes, pero si no diseña y administra cuidadosamente un programa de restablecimiento contra desastres para su compañía, no realiza su trabajo de manera correcta. La importancia de esta área no puede pasarse por alto. Además de este capítulo, usted también debe estudiar el material que aborda las instrucciones específicas acerca del restablecimiento y respaldo de sus sistemas operativos de red y sus bases de datos, así como la documentación del dispositivo hardware y software de respaldo que haya seleccionado.

El capítulo siguiente analiza información clave que debe saber acerca de la selección, instalación y administración de servidores, los cuales son el corazón de la red; de manera que una selección de servidores confiables y productivos no solamente eliminará problemas potenciales de su red, sino que podrán ayudarle a evitar que use, de hecho, los planes y las estrategias de restablecimiento contra desastres que usted ha diseñado.

CAPÍTULO 13

Servidores de red: todo lo que quería saber, pero temía preguntar

Existe una gran cantidad de tipos diferentes de servidores, como de archivo e impresión, de aplicaciones, de web y más. Sin embargo, lo que todos los servidores tienen en común es que la gente depende de ellos y que, en general, son parte integral de algún tipo de servicio de red. Debido a que son utilizados por decenas o centenas (¡o miles!) de personas, las computadoras que usted utiliza como servidores necesitan ser una superior —o duplicar— cualquier otra estación de trabajo antigua. Los servidores necesitan ser más confiables y serviciales que las estaciones de trabajo. Además, deben hacer su trabajo de forma diferente a éstas.

En este capítulo usted aprenderá acerca del hardware del servidor de la red. Además, sobre lo que distingue a un servidor de una estación de trabajo, las diferentes configuraciones de hardware del servidor y la preparación de un servidor para utilizarse en su red.

DIFERENCIAS ENTRE UN SERVIDOR Y UNA ESTACIÓN DE TRABAJO

Debido a que el costo de las computadoras de escritorio de alto desempeño es de 1500 a 3000 dólares, puede ser difícil explicarse por qué una computadora con el mismo procesador puede costar más de 10000 dólares solo porque está diseñada para ser un "servidor". Sin embargo, las computadoras servidores en verdad son diferentes de las estaciones de trabajo, pues incorporan un gran número de características importantes que no se encuentran en las computadoras de escritorio y que son importantes para la función de un servidor, como proporcionar datos o servicios a un gran número de usuarios de la manera más confiable posible.

Procesadores de servidor

Una gran parte del desempeño de un servidor se basa en su *unidad central de proceso* o CPU. A pesar de que los servidores son muy sensibles al desempeño de otros componentes (más que al de una computadora de escritorio), el procesador es aún más importante para determinar la velocidad del servidor.

Los servidores pueden operar mediante el empleo de uno o muchos procesadores. Con cuántos procesadores deberá usted seleccionar un servidor, dependerá de muchos factores. El primero es el sistema operativo de red (NOS) que utilice. Usted deberá investigar con mucho cuidado cuántos procesadores soporta su NOS si desea utilizar multiprocesamiento.

Si usted planea utilizar Windows 2000 Server o Windows Server 2003, puede utilizar procesadores múltiples, lo que dependerá de qué edición de esos NOS planee instalar. Windows 2000 Server puede manejar hasta cuatro procesadores, mientras que Windows 2000 Advanced Server puede soportar hasta ocho procesadores y Windows 2000 Datacenter Server hasta 32. En el caso de Windows Server 2003, tanto la edición Estándar como la Web soportan hasta 2 procesadores, la edición Enterprise maneja hasta 8 y la edición Datacenter hasta 32 (y hasta 128 en la versión de 64 bits). Si usted planea utilizar UNIX, entonces depende, pues algunas versiones de UNIX soportan múltiples procesadores mientras que otras no.

Otro factor que debe considerar es el trabajo que realiza el servidor y si las tareas del mismo representan en este momento un cuello de botella para el procesador. Los servidores de archivo y de impresión pueden operar sin procesadores múltiples. A pesar de que se benefician de pro-

cesadores rápidos, la ventaja no es tan grande como usted podría pensarlo. Por el contrario, en el caso de un servidor de archivos o de impresión, es mucho más importante que tenga una gran cantidad de RAM y un subsistema de disco muy veloz. Por otro lado, los servidores de bases de datos consumen muchísima capacidad del procesador y en definitiva se beneficiarán de tantos procesadores como sea posible que operen a la máxima velocidad posible. (También es importante que el software del servidor de la base de datos se configure de forma que pueda hacer un uso óptimo de los múltiples procesadores). Los servidores web tienden a ser modestos en cuanto a sus requerimientos de procesamiento pues dependen de buses rápidos, conexiones de red más rápidas, mucha RAM, discos rápidos y eso es todo. Un procesador rápido (o múltiples procesadores) es perfecto para la mayoría de los servidores web, pero también podría estar subutilizado.

La administración de múltiples procesadores requiere mucho trabajo del sistema operativo. Debido a esto, tener el doble de procesadores en una computadora no duplica su capacidad de procesamiento; por el contrario, duplicar los procesadores puede mejorar la velocidad de la computadora solo 50%. Dependiendo de su sistema operativo, existe también un punto de poca ganancia, que una vez superado, aunque se agreguen más procesadores, el desempeño no mejorará en forma significativa. Esta aparente contradicción está relacionada, en forma parcial, con la forma en que los procesadores múltiples manejen el sistema operativo. Otra parte tiene que ver con el número de mezclas que realiza el trabajo en un sistema operativo. (Las mezclas no pueden compartirse entre procesadores, por lo que si solo dos mezclas principales hacen todo el trabajo, más de dos procesadores no mejorarán su desempeño en una forma significativa).

Para determinar el número de procesadores que usted deberá utilizar para realizar cualquier tarea, debe consultar con el fabricante del sistema operativo de red que planea utilizar y con los fabricantes de las aplicaciones principales que desee correr en el servidor. Es probable que también le convenga consultar estos aspectos con otras compañías que realicen trabajos similares con la aplicación del servidor propuesto. Por ejemplo, para un servidor de base de datos de un sistema contable que soporte a cientos de usuarios, deberá hablar con otras compañías que utilicen el mismo software y que cuenten, aproximadamente, con el mismo número de usuarios, a fin de aprender acerca de sus experiencias y sugerencias. Es muy importante revisar dos veces las

¡DEFÍNALO! ¿Qué es una mezcla?

A menudo, los sistemas operativos multitarea realizan su función mediante un mecanismo llamado *mezcla*. En realidad, todos los sistemas operativos modernos utilizan mezclas, entre ellos Windows 9x, Windows NT/2000/XP, OS/2, NetWare y muchas versiones de UNIX. En los sistemas operativos que utilizan mezclas, cada programa corre como un proceso, el cual tiene sus recursos de memoria propios y se mantiene separado de los demás procesos en la computadora. Sin embargo, el proceso se divide en diferentes unidades de trabajo llamadas mezclas, las cuales tienen acceso a todos los recursos del proceso en el que corren y son los "agentes de trabajo" reales dentro de éste. Por ejemplo, un procesador de palabra como Microsoft Word puede tener una mezcla principal que acepte información tecleada por parte del usuario y la despliegue en la pantalla, otra que maneje cualquier trabajo de impresión y otras que verifiquen de manera constante la ortografía y la gramática tras bambalinas a medida que los usuarios lleven a cabo sus tareas. En este ejemplo, la aplicación Word es un solo proceso con múltiples mezclas. En un sistema operativo multimezcla, cada proceso tiene al menos una mezcla siempre.

configuraciones propuestas del servidor de esta forma, ya que sus diferentes usos requieren más —o mucho menos— recursos de hardware que los que pueda calcular. Si usted puede encontrar otra compañía que haga lo mismo y aproximadamente con la misma carga de trabajo, podrá sentirse mucho más seguro de que la configuración propuesta del hardware del servidor satisfará sus necesidades.

La familia Pentium de Intel

La familia Pentium de Intel ofrece una gran variedad de procesadores, desde el Pentium básico hasta el procesador Pentium 4 Xeon. Las actuales computadoras tipo servidor se entregan con procesadores Pentium 4 o Pentium 4 Xeon. La serie de procesadores Xeon está optimizada para realizar tareas tipo servidor y es más adecuado para correr en un sistema de multiprocesamiento.

Los procesadores Pentium 4 Xeon se encuentran actualmente disponibles con velocidades que varían desde 1.4 GHz hasta 3.6 GHz. El diseño del procesador Xeon acepta de 8 a 32 procesadores en un sistema Pentium 4 Xeon. Para ciertas aplicaciones, tener un número tan grande de procesadores puede representar una ventaja. La familia de procesadores Xeon está ensamblada como un cartucho de contacto de una sola orilla, la cual es mayor que el ensamblado que se utilizó en los procesadores Pentium Non-Xeon. Los procesadores Xeon también generan mucho más calor que sus equivalentes Non-Xeon, debido principalmente a la memoria caché que es más grande y a otras características que mejoran el desempeño del procesador Xeon en un servidor. (Es deseable que la mayoría de los servidores puedan supervisar sus niveles de calor dentro de su ensamblaje; a veces, estos chips pueden calentarse a más de 170º Fahrenheit).

El siguiente gran paso en procesadores para servidor de Intel proviene de su nueva familia de procesadores Itanium, conocida antes como la arquitectura IA64. La familia Itanium se basa en una arquitectura de 64 bits que utiliza algo que Intel llama EPIC (Explicitly Parallel Instruction Computing). Los procesadores Itanium 2 se encuentran actualmente disponibles a velocidades que van desde 1.0 hasta 1.6 GHz. En gran medida, esta arquitectura depende de las técnicas de compilación para arreglar el código en el nivel byte, de forma que pueda ejecutarse en paralelo de la forma más eficiente posible (lo que significa que múltiples instrucciones del procesador se ejecuten al mismo tiempo).



NOTA Usted, en general, no puede comparar la velocidad del reloj de los procesadores de una familia con la velocidad del reloj de los de otra familia con el fin de tener una idea de su desempeño relativo. Los procesadores de las diferentes familias y de fabricantes diferentes trabajan en formas muy distintas. Lo que a una familia de procesadores le toma cuatro a seis ciclos de instrucción en realizar, podría tomarle a otra familia solo un ciclo de instrucción. En lugar de lo anterior, utilice las velocidades del reloj para darse una idea de la diferencia relativa de velocidades entre procesadores solo de una misma familia.

Clones de Intel

Advanced Micro Devices (AMD) fabrica la línea de procesadores Athlon, la cual compite principalmente con los Pentium III y 4 y, en esencia, emula el funcionamiento de la familia de procesadores Intel. En los dos últimos años, AMD ha tenido éxito en producir procesadores que rivalizan con los de Intel, pero, en muchos casos, éstos los superan.

El problema con los chips clonados como los de AMD es que, a pesar de que se diga lo contrario, nunca serán totalmente compatibles con los procesadores de Intel. Debido a que los fabricantes de software, en general, certifican su software solo contra procesadores Intel, es seguro

que responderán de manera muy lenta ante cualquier problema que llegara a suscitarse con los clones. Debido a esta circunstancia, los chips clonados por lo general no se utilizan en las computadoras tipo servidor, donde la confiabilidad y el servicio son de gran importancia. Por el contrario, los procesadores AMD son una buena elección para muchas computadoras de escritorio y, a menudo, éstas son ligeramente menos caras que sus equivalentes basadas en Intel.



PISTA Antes de seleccionar cualquier hardware de servidor, asegúrese de que el fabricante del software de red que usted planea utilizar, certifique todo el sistema, incluyendo el procesador. Además, es muy importante asegurarse de que el fabricante de cualquier aplicación que usted planee correr en el servidor certifique también el hardware que usted haya seleccionado. (La mayoría de los fabricantes de aplicaciones para servidores insisten solo en que el hardware esté certificado para el sistema operativo, pero es muy recomendable realizar la doble verificación).

PowerPC

Originalmente, Motorola, IBM y Apple formaron un grupo para diseñar y utilizar el procesador PowerPC, basado en la arquitectura RISC que es, en realidad, fabricado por Motorola que se basaba más que nada en el diseño de IBM. En la actualidad, el PowerPC se utiliza en las computadoras Macintosh, de Apple, y en algunos servidores de IBM y Motorola basados en UNIX. Si usted corre una red basada en Macintosh, puede estar casi seguro de que está utilizando el procesador PowerPC tanto en sus computadoras de escritorio como en cualquier servidor fabricado por Apple.

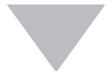
Capacidades de bus

En la mayoría de los servidores, el nombre del juego es mover datos, generalmente, muchos datos. Los servidores de archivo e impresión necesitan dar servicio a cientos de archivos de manera simultánea, a cientos de usuarios y coordinar y manejar las necesidades de datos de todos ellos. Los servidores de bases de datos deben administrar bases con capacidades de muchos gigabytes o terabytes y deben ser capaces de recuperar una gran cantidad de datos de sus bases y proporcionarlos a los usuarios en cuestión de milisegundos. Los servidores de aplicaciones deben llevar a cabo operaciones de uso intenso tanto del procesador como del disco, y a la vez proporcionar servicios de aplicación a los usuarios.

De la misma forma en que a menudo las redes tienen segmentos de espina dorsal rápidos que conectan muchos segmentos más lentos, una computadora depende de su bus para hacer el mismo tipo de trabajo. Un bus es la “espina dorsal” de la transferencia de datos de un sistema de cómputo, al que se conectan el procesador, la memoria y todos los demás dispositivos instalados. En cualquier momento dado, un servidor puede transferir megabytes de datos desde sus discos hacia las tarjetas de red, hacia el procesador, hacia la memoria del sistema y de regreso a los discos a medida que lleve a cabo sus tareas. Todos estos componentes están conectados entre sí por el bus del sistema, por lo que es muy importante optimizar al máximo esa parte de la computadora. En realidad, el bus debe manejar aproximadamente cinco veces más datos que cualquier otro componente del sistema, y necesita hacerlo de la forma más rápida posible. Mientras que es verdad que un bus PCI moderno puede manejar 33 MHz a 32 bits, este nivel no es suficiente en un servidor de alta capacidad. Muchos servidores pueden manejar múltiples NIC (cada una a velocidades de hasta 100 Mbps o de 1 Gbps) y múltiples controladores de disco que corran a velocidades de hasta 40 Mbps. Si dichos dispositivos se encuentran ocupados al mismo tiempo, incluso un bus PCI se saturará rápidamente.

Por tanto, los fabricantes de servidores deben vencer las limitaciones relativas a la velocidad de bus. Los fabricantes utilizan varios esquemas para hacerlo. Una forma es utilizar múltiples buses en un solo sistema. Por ejemplo, algunos servidores NetServer de HP utilizan tres buses PCI que puedan trabajar todos a máxima velocidad de manera simultánea. Si usted aplica solo un poco de planeación cuando coloca ciertos periféricos en buses diferentes, podrá incrementar de una forma significativa la velocidad total del sistema.

Un consorcio de fabricantes de hardware, que incluye a Compaq, HP, IBM, Dell y muchos otros, ha utilizado también una mejora a PCI llamada PCI Express. Esta versión l PCI Express proporciona un bus de 133 MHz a 64 bits o hasta 1 066 MBps de desempeño (sí, megabytes por segundo).

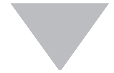


NOTA El PCI Express (antes llamado PCI-X) se ha diseñado para que sea compatible con versiones anteriores del estándar PCI, utilizando una tarjeta PCI más lenta en el bus del PCI Express para reducir su velocidad. No obstante, se espera que dichos sistemas soporten tanto un bus PCI estándar para tarjetas PCI como un bus PCI Express para tarjetas PCI Express.

También se han llevado a cabo otras mejoras al bus. En la actualidad existe un estándar de bus de alta velocidad que se llama "Infiniband", el cual incorpora el trabajo de otros proyectos llamados System I/O y Next Generation I/O. Infiniband utiliza un método conmutado y puede manejar hasta 6 Gbps entre cualquier par de nodos conectados.

RAM

Otra parte importante de cualquier servidor es su memoria. Los servidores dependen en gran medida de su capacidad de almacenar datos desde la red y desde los discos del servidor para lograr el mejor desempeño posible. Para llevar a cabo esta tarea, dependen en gran medida de su memoria de acceso aleatorio (RAM). Por ejemplo, la mayoría de los sistemas operativos de red almacenan en su memoria caché todo el directorio de archivos para su rápido acceso. Asimismo, guardan los archivos requeridos en la memoria caché por un periodo extenso en caso de que los datos que contienen se necesiten otra vez. Además, escriben en el disco del sistema mediante la escritura de la RAM y llevan a cabo las escrituras en el disco real de manera asíncrona, por lo que los discos no representan un cuello de botella como lo serían de otra forma. En la mayoría de los servidores, 512 MB de RAM se considera el mínimo aceptable. En servidores de bases de datos de gran capacidad que soportan a cientos de usuarios, usted debe instalar más de 1 GB de RAM a fin de lograr el mejor desempeño posible.



PISTA En realidad, ¿qué cantidad de RAM necesita para su servidor? Esto es difícil de determinar ya que mucho depende de cómo se utilice el servidor. La buena noticia es que tanto la familia de servidores de Windows (de Windows NY a Windows Server 2003) y NetWare de Novell proporcionan estadísticas que muestran cómo se utiliza la memoria en el sistema. Usted puede utilizar esta información a fin de ayudar a determinar cuándo será conveniente contar con más memoria. En la familia Windows de sistemas operativos para servidor, utilice el Performance Monitor para ver cómo se utilizan la memoria y el archivo de intercambio del sistema. En NetWare de Novell, emplee las estadísticas de la memoria caché del programa MONITOR de la consola.

La memoria RAM se presenta en tres variedades: sin paridad, con paridad y con verificación y corrección de errores (ECC). La RAM con paridad utiliza un bit extra en cada byte para almacenar la suma verificadora del contenido del byte. Si la suma verificadora no coincide con la memoria leída, el sistema se detiene y se reporta un error en la memoria. La memoria sin paridad elimina el bit de paridad y, por tanto, no detecta ningún error en la memoria. A veces, las computadoras de escritorio baratas utilizan la memoria RAM sin paridad como una forma de reducir los costos, aunque se debe evitar su uso siempre que sea posible, aun en computadoras de escritorio.

La memoria con paridad tiene dos problemas. Primero, el sistema solo puede detectar errores en la memoria, es decir, no puede corregirlos. Segundo, debido a que solo se utiliza un bit para almacenar la paridad, es posible "engañar" al mecanismo de paridad con un error más severo. Por ejemplo, si dos bits cambian de polaridad de manera simultánea, el sistema de paridad no detectará el problema. La memoria ECC está diseñada para resolver estos problemas. Los sistemas que utilizan la memoria ECC pueden detectar hasta dos bits en error y automáticamente corregirlo. La mayoría de los servidores actuales utilizan la memoria ECC debido a la protección adicional que ésta ofrece.

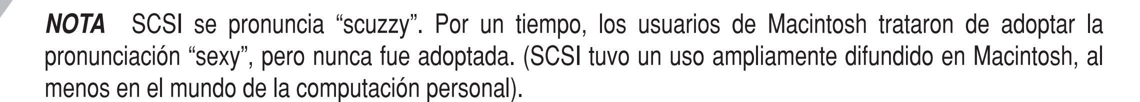
Otro tipo de RAM es la memoria dinámica de acceso aleatorio Rambus (RDRAM). La RDRAM es más rápida que otros tipos de RAM. Debido a que se presentaron algunos problemas iniciales con las tarjetas madre basadas en RDRAM, Intel y Rambus al parecer tienen los enredos resueltos en cuanto a la RDRAM, y se puede esperar que ésta se utilice más ampliamente en servidores. Sin embargo, en la actualidad, la mayoría de los servidores se venden con la memoria RAM síncrona dinámica (SDRAM), la cual se piensa que es más confiable y consistente que la RDRAM, y también es mucho más barata.

Subsistemas del disco

El tercer subsistema crucial del desempeño de un servidor son sus controladores de disco. Los controladores del disco duro son, en general, los componentes más lentos de cualquier sistema y, debido a que la mayoría del trabajo del servidor involucra a los discos duros, representan los componentes del sistema donde existe la mayor probabilidad de que se presenten cuellos de botella. Asimismo, los datos almacenados en un servidor son, en general, de importancia crítica para la compañía, por lo que es importante tener la configuración de disco más confiable posible.

Interfases del disco: SCSI versus SATA

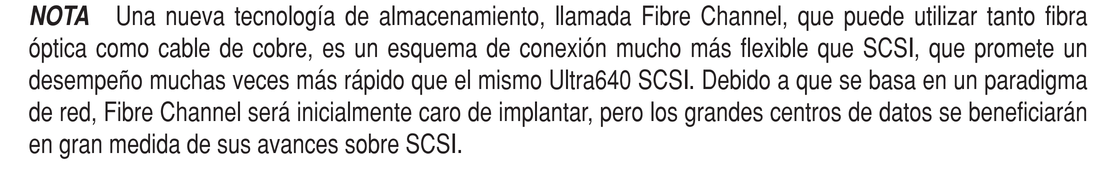
En la actualidad existen dos tipos de interfaz de disco que tienen un amplio uso: Conexión Serial de Tecnología Avanzada (SATA) e Interfase para Sistemas de Cómputo Pequeños (SCSI). En una estación de trabajo que utilice Windows XP, el desempeño de SATA está muy a la par con los sistemas de disco basados en SCSI. Sin embargo, en el caso de un servidor que corre Windows o NetWare de Novell, el desempeño de SCSI ofrece grandes ventajas. Está más allá del alcance de esta sección analizar todos los detalles que distinguen a SATA de la SCSI. Sin embargo, los sistemas SCSI se desempeñan mucho mejor cuando tienen acceso simultáneo a más de un disco duro y cuando se utilizan en un sistema operativo —como NetWare, la familia de servidores de Windows, o aun UNIX— que pueden aprovechar las ventajas de las características de la interfase SCSI.



NOTA SCSI se pronuncia "scuzzy". Por un tiempo, los usuarios de Macintosh trataron de adoptar la pronunciación "sexy", pero nunca fue adoptada. (SCSI tuvo un uso ampliamente difundido en Macintosh, al menos en el mundo de la computación personal).

Existen muchas variedades de sistemas de disco basadas en SCSI que se encuentran disponibles, a saber:

- **SCSI-1** La especificación básica de SCSI puede transferir datos hacia y desde los discos a 5 MBps aproximadamente utilizando un ancho de transferencia de 8 bits. Los avances en la tecnología de SCSI han hecho caer en la obsolescencia a SCSI-1, por lo que no se utiliza en los sistemas actuales. (Lo anterior es bueno ya que la mayoría de las implantaciones con SCSI-1 no eran compatibles entre sí).
- **SCSI-2** Ésta es la interfase básica en uso en la actualidad. Amplía la especificación SCSI, agrega muchas características a SCSI y también permite conexiones más rápidas. Además, SCSI-2 mejora en gran medida la compatibilidad entre los diferentes fabricantes de dispositivos SCSI.
- **Fast-SCSI** Con la Fast-SCSI, la especificación básica SCSI-2 es mejorada a fin de incrementar la velocidad del bus SCSI de 5 MHz a 10 MHz y el desempeño de 5 MBps a 10 MBps. A la Fast-SCSI también se le conoce con el nombre de *Fast Narrow-SCSI*.
- **Wide-SCSI** También con base en SCSI-2, Wide-SCSI incrementa la trayectoria de datos de SCSI-2 de 8 a 16 ó 32 bits. Cuando utiliza 16 bits, Wide-SCSI puede manejar hasta 20 MBps.
- **Ultra-SCSI** También llamada SCSI-3, esta especificación incrementa la velocidad del bus SCSI aún más: a 20 MHz. Cuando utiliza un bus de 8 bits angosto, Ultra-SCSI puede manejar 20 MBps. También puede correr con una bus de 16 bits, con lo cual incrementa la velocidad a 40 MBps.
- **Ultra2 SCSI** También una mejora del estándar SCSI, Ultra2 SCSI duplica (de nuevo) el desempeño de la Ultra-SCSI. Los subsistemas de Ultra2 SCSI pueden escalar hasta 80 MBps si utilizan un bus de 16 bits.
- **Ultra160 SCSI** A estas alturas, debe conocer la historia: Ultra160 SCSI de nuevo duplicó el desempeño de Ultra2 SCSI. Ultra160 SCSI (que anteriormente se llamaba Ultra3 SCSI) se denomina así por su desempeño de 160 MBps.
- **Ultra320 SCSI** Es un estándar que comienza y transferirá datos a 320 MBps.
- **Ultra640 SCSI** Este estándar, que fue lanzado como nuevo a principios del año 2003, duplica la velocidad de la interfase SCSI.


NOTA Una nueva tecnología de almacenamiento, llamada Fibre Channel, que puede utilizar tanto fibra óptica como cable de cobre, es un esquema de conexión mucho más flexible que SCSI, que promete un desempeño muchas veces más rápido que el mismo Ultra640 SCSI. Debido a que se basa en un paradigma de red, Fibre Channel será inicialmente caro de implantar, pero los grandes centros de datos se beneficiarán en gran medida de sus avances sobre SCSI.

Como puede observar en la lista anterior, un enorme conjunto de opciones de SCSI están disponibles en el mercado en la actualidad. Debido a todos los diferentes estándares, es una buena idea asegurase de que adquiera componentes compatibles cuando construya un subsistema de discos SCSI o cuando compre uno como parte de un servidor. Asegúrese de que la tarjeta

controladora que usted planea utilizar sea compatible con los controladores que vaya a usar, que tenga los cables adecuados y que sea compatible tanto con la computadora del servidor como con el sistema operativo de red que usted desee instalar. La buena noticia es que una vez que logre tener el subsistema de discos SCSI trabajando, lo hará de manera confiable y con un desempeño excelente.

Topologías de disco: ¡Es un RAID!

Las siglas *RAID* quieren decir arreglo redundante de discos baratos. RAID es una técnica que consiste en utilizar muchos discos para hacer el trabajo de un solo disco, y proporciona muchas ventajas comparado con la utilización de un número menor de discos de mayor tamaño.

La idea fundamental del RAID radica en redistribuir los datos del servidor en muchos discos, de manera transparente. Por ejemplo, un solo archivo puede tener porciones de sí mismo dispersos en cuatro o cinco discos. El sistema RAID administra todas esas partes de forma que usted nunca se entera de que, en realidad, el archivo se encuentra en todos los discos. Usted abre el archivo, el sistema RAID accede a todos los discos correspondientes y lo "ensambla" y lo pone a su disposición.

El beneficio inmediato que obtiene es que los múltiples discos hacen el trabajo más rápido que uno solo. Esta característica se debe a que todos los discos pueden trabajar de manera independiente en la búsqueda de sus propios datos y el envío de éstos hacia el controlador a fin de que sean ensamblados. Un solo controlador de disco estaría limitado por una sola cabeza en el disco y le tomaría mucho más tiempo reunir la misma cantidad de información. De forma sorprendente, el desempeño de un sistema RAID *aumenta* a medida que agregan más discos, debido al beneficio que se obtiene cuando todas esas cabezas del disco trabajan de manera independiente en la recuperación de los datos necesarios.

Si usted piensa en un solo arreglo RAID con los datos dispersos en muchos discos, probablemente notará que, a la vez que mejora el desempeño, también aumenta la probabilidad de que un disco falle. Utilizar cinco discos que hagan el trabajo de uno solo significa que existe una probabilidad cinco veces mayor de que un disco falle. Debido a que los datos están dispersos en todos los discos, si uno falla, perderá los datos contenidos en los discos restantes, ya que no serán útiles si se pierde una gran parte de los datos. Por fortuna, los diferentes esquemas de RAID resuelven este problema, como podrá observar en el análisis siguiente.

Existen muchas maneras de utilizar múltiples discos juntos en algún tipo de esquema RAID y, de acuerdo con este punto de vista, se definen varios *niveles RAID*, cada uno de los cuales describe una técnica diferente, como sigue:

- **RAID 0** Este esquema es una configuración por medio de la cual los datos se dividen (*se descomponen*) en múltiples discos, pero *sin redundancia*. La pérdida de un controlador en un arreglo RAID 0 provoca la pérdida de datos en todos los discos. El RAID 0 es apropiado solo para mejorar el desempeño y deberá utilizarse únicamente con datos que no sean muy importantes. Los arreglos RAID 0 pueden dividir los datos en dos o más discos, como se muestra en la figura 13-1.

- **RAID 1** Este tipo de arreglo no divide los datos en múltiples discos. En lugar de ello, define un estándar por medio del cual los datos se respaldan en los discos. Se utilizan dos discos en lugar de uno y los datos se mantienen sincronizados entre los dos discos. Si uno de éstos falla, el disco restante continúa trabajando de manera normal hasta que el que falló sea reemplazado. A menudo, RAID 1 se conoce con el nombre de *espejo*.

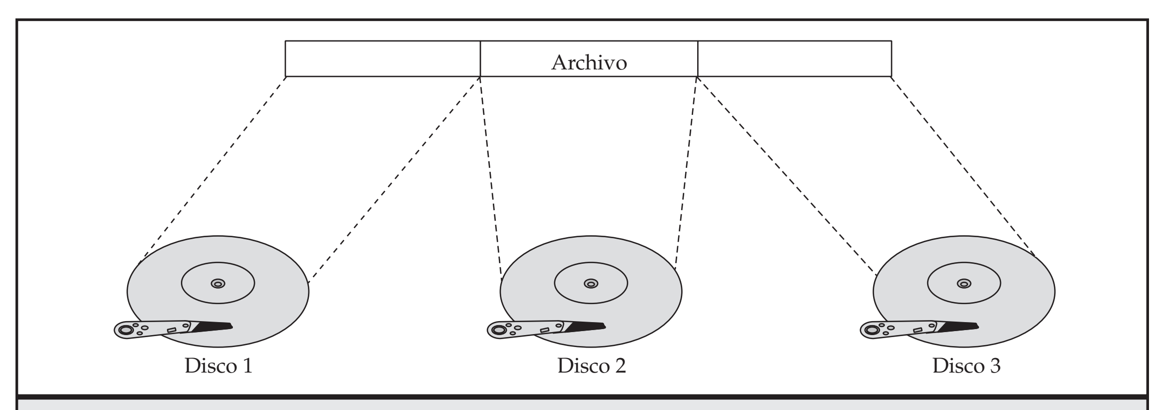
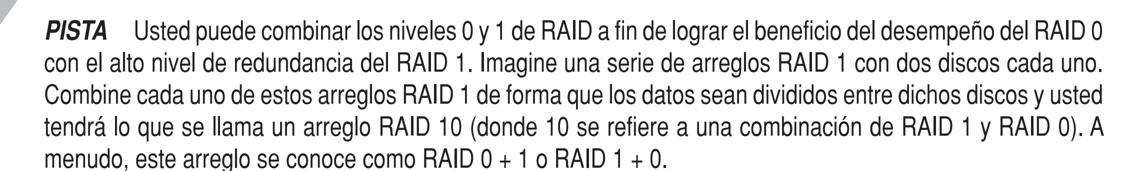


Figura 13-1. Un arreglo RAID 0 distribuye los datos en múltiples discos.

Una mejora del RAID 1 se conoce como *duplexaje*: los datos están duplicados también en dos discos, pero cada uno tiene su propio controlador, lo cual le agrega otro nivel de redundancia (ya que usted puede perder tanto un disco como un controlador y, a pesar de esto, seguir trabajando). El duplexaje también puede mejorar el desempeño de alguna manera en comparación con el espejeo. Algunas implantaciones RAID 1 son lo suficientemente inteligentes para leer datos desde cualquier disco de forma que cualquiera de los discos que tenga su cabeza de controlador más cerca de los datos realizará la solicitud de lectura, mientras que el otro permanecerá ocioso. Sin embargo, todas las escrituras deben ocurrir de manera simultánea en ambos discos. La figura 13-2 muestra un dibujo de un arreglo RAID 1 típico.



PISTA Usted puede combinar los niveles 0 y 1 de RAID a fin de lograr el beneficio del desempeño del RAID 0 con el alto nivel de redundancia del RAID 1. Imagine una serie de arreglos RAID 1 con dos discos cada uno. Combine cada uno de estos arreglos RAID 1 de forma que los datos sean divididos entre dichos discos y usted tendrá lo que se llama un arreglo RAID 10 (donde 10 se refiere a una combinación de RAID 1 y RAID 0). A menudo, este arreglo se conoce como RAID 0 + 1 o RAID 1 + 0.

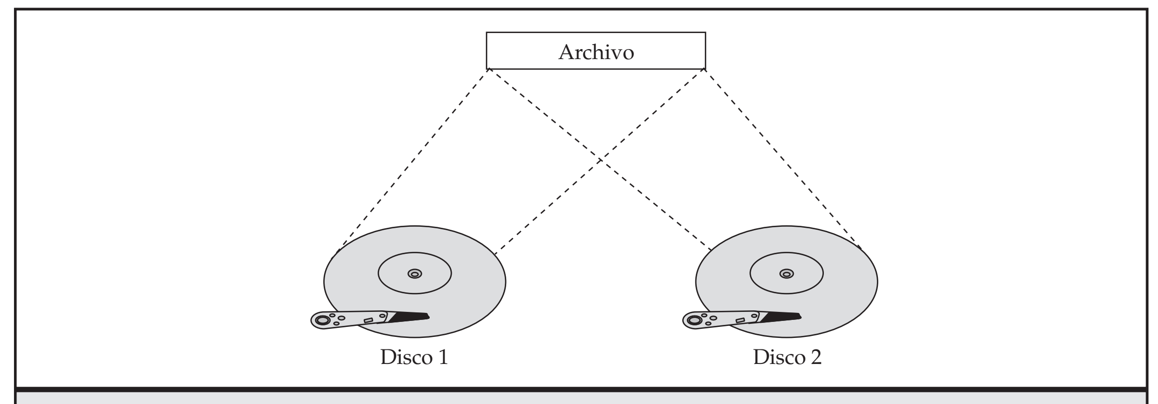


Figura 13-2. Un arreglo RAID 1 duplica los datos en dos discos.

- **RAID 2** Es probable que usted no vea el RAID 2 implantado en el mundo real. RAID 2 es una especificación técnica que divide los datos en múltiples discos y después utiliza una código Hamming ECC que está escrito en un conjunto de discos ECC. El cociente entre el número de discos de datos y el de discos ECC es muy alto en RAID 2: hay cuatros discos de datos por cada tres discos ECC. El RAID 2 no se utiliza debido a que no es eficiente.

- **RAID 3** Aquí es donde RAID se comienza a poner interesante; las implantaciones de RAID 3 solían ser muy comunes, aunque en estos días usted puede ver que RAID 5 se utiliza mucho más que éste que divide los datos en múltiples discos y, después, utiliza una operación OR exclusiva (XOR) a nivel bit en todos los datos almacenados en cada disco que tenga datos ECC, los cuales se escriben en un solo controlador ECC. Así que, por ejemplo, usted puede tener cuatro controladores de datos y un controlador ECC para respaldarlos. La figura 13-3 muestra un arreglo RAID-3. Los datos XOR tienen una propiedad matemática interesante. Si usted quita uno de los controladores de datos, puede tomar los datos restantes, más los que contiene el controlador ECC, y reconstruir lo que se ha perdido a partir del disco que falle. Los controladores del disco RAID hacen esta tarea de manera automática en el caso de que un controlador falle, aunque los controladores trabajen a una velocidad mucho más baja que la normal debido al tiempo desperdiciado en tener que reconstruir los datos a medida que viajan. Una técnica mucho más útil es reemplazar el disco que falla y, después, utilizar los datos ECC para reconstruir los datos perdidos.

NOTA Si más de un controlador se pierde de un arreglo RAID 3 o uno RAID 5, todos los datos del arreglo se perderán. Aun así, estos arreglos ofrecen una buena protección a un costo incremental relativamente bajo.

- **RAID 4** Éste es otro de los estándares de RAID que no se utiliza mucho en el mundo real. El RAID 4 es similar al RAID 3, excepto que los datos no se dividen entre los diferentes controladores de datos. En lugar de eso, cada bloque de datos se escribe por completo en un solo controlador de datos, y el siguiente bloque se escribe en el controlador de datos siguiente, y así sucesivamente. El RAID 4 aún utiliza un solo disco ECC para todos los controladores de datos, pero en general es muy ineficiente para aportar un beneficio, particularmente cuando se lo compara con el RAID 3.

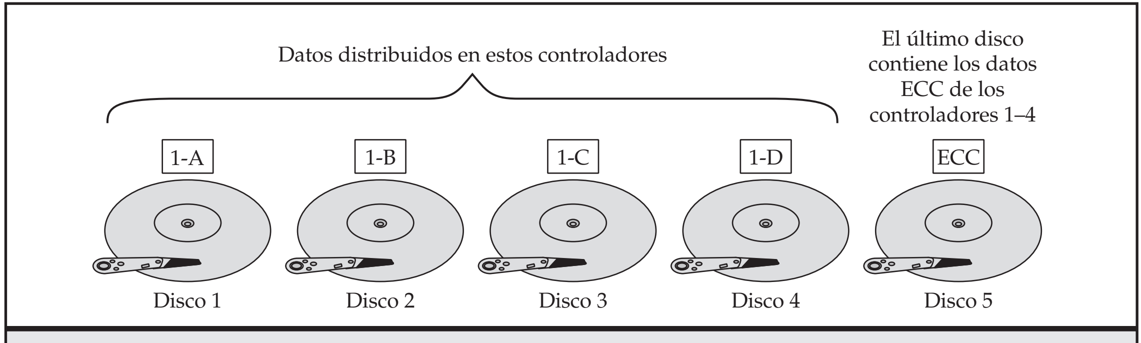


Figura 13-3. Un arreglo RAID-3 distribuye los datos en múltiples discos, con un disco ECC para proteger los datos.

▲ **RAID 5** El RAID 5, que se muestra en la figura 13-4, es el estándar actual de los sistemas RAID. (El RAID 1 también es un estándar actual, pero tiene diferentes aplicaciones). Recuerde cómo trabaja el RAID 3, con los datos divididos en un conjunto de discos de datos y el código ECC escrito en un solo disco ECC. El RAID 5 mejora este esquema pues intercala los datos y la información ECC en todos los discos. La gran ventaja de este método respecto a RAID 3 es que no depende de un solo controlador ECC para todas las operaciones escritas, lo cual se convierte en un cuello de botella en los sistemas RAID 3. Debido a que todos los controladores comparten el trabajo del ECC, el desempeño del RAID 5 es ligeramente mejor que el del RAID 3. Aunque existe una pequeña desventaja que la mayoría de las personas pasa por alto. En los sistemas RAID 3, si usted pierde el controlador de datos, el sistema trabaja más lento (generalmente la velocidad disminuye de manera dramática) puesto que los datos se reconstruyen de pasada. Sin embargo, si pierde el controlador ECC, el sistema aún operará tan rápido como si no se hubiera perdido el controlador. En el caso del sistema RAID 5, si pierde un controlador, usted estará siempre perdiendo parte de su controlador ECC (ya que su tarea se divide entre todos los discos) y el desempeño se deteriora.

PISTA Los fabricantes de servidores le dan mucha importancia a la forma en que permitirá el diseño de un sistema RAID 5 continuar trabajando si el controlador falla. Mientras que esta inquietud es válida desde el punto de vista técnico, el desempeño de un servidor en esa condición es más pobre que lo esperado, posiblemente tan pobre que nadie querrá usar el servidor. Sin embargo, el RAID 5 es excelente para reconstruir los datos perdidos una vez que es reemplazado el controlador que fallaba. Mientras que completar este proceso puede emplear algunas horas, le puede proporcionar un sentimiento de confort. Este proceso puede hacer que no pierda datos y que no tenga que restablecer el sistema a partir de un respaldo en cinta reciente, lo cual usted tendría que llevar a cabo si no tuviera algún nivel de protección RAID en su servidor.

¿Qué nivel de RAID deberá utilizar en su servidor de red? La mayoría de los administradores de red prefieren RAID 5 debido a que este requiere solo entre 20 y 25% de la capacidad total del disco para la función de redundancia. Sin embargo, trabaja bien y ofrece una medida de seguridad. Sin embargo, en ocasiones, los arreglos RAID 3 y RAID 5 tienen problemas en la recu-

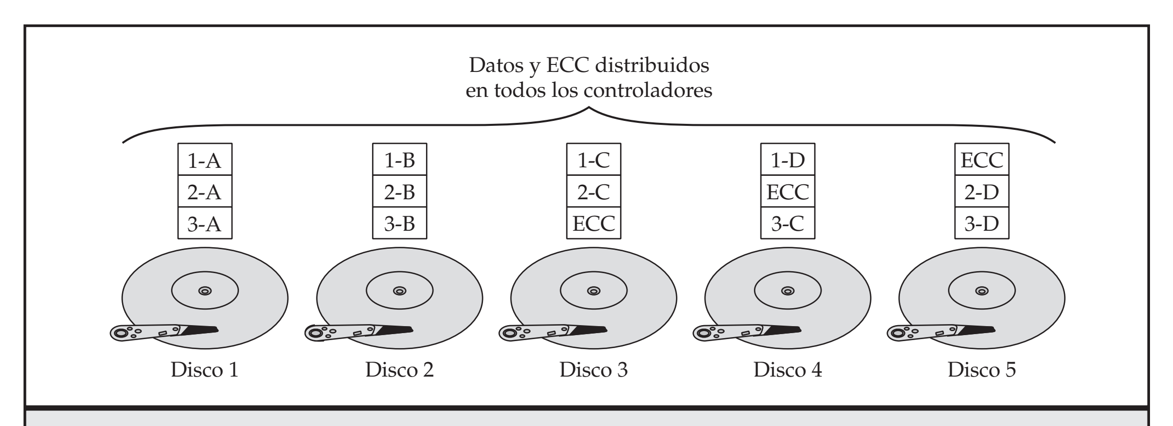


Figura 13-4. Un arreglo RAID 5 distribuye los datos en múltiples discos y, de manera alternativa, utiliza todos los discos de los datos ECC.

peración adecuada de los datos (aunque muy de vez en cuando los pierden). Por esta razón, en general usted debe optar ya sea por RAID 1 o RAID 10 para los servidores de red que almacenan datos importantes.

En general, las diferentes configuraciones de RAID ofrecen distintos niveles de confiabilidad. Si se les otorga un valor desde el mejor hasta el peor en términos solo de la probabilidad del sistema de perder datos, en primer lugar estaría el RAID 1, luego el RAID 10 y después el RAID 5 y el RAID 3. Aunque siempre existen intercambios. Un sistema de 20 discos que utilice solo RAID 1 sería muy difícil de manejar, ya que usted tendría 10 controladores lógicos que administrar y utilizar de manera eficiente. Sin embargo, si configura esos mismos 20 discos y forma dos arreglos RAID 5, podrá administrar de una manera más eficiente los dos discos lógicos que resultarían.

Usted deberá tomar una decisión con base en la importancia de los datos, los niveles de desempeño requeridos, las capacidades del servidor y el presupuesto que le asignen. Sin embargo, ¡una cosa que nunca deberá hacer es confiarse de que cualquier nivel de RAID reemplaza los respaldos en cinta de los datos que se hacen regularmente!

I2O

Abreviatura de I/O Inteligente, el I2O (a menudo escrito como I2O) es un estándar emergente que transfiere el procesamiento I/O desde el procesador de la computadora hasta el controlador del disco. I2O promete mejorar de alguna forma el desempeño de los subsistemas de discos, aunque no tanto como sus promotores lo sugieren. Al final del día, el procesamiento I/O estará hecho de todos modos; estará hecho en el controlador de disco del I2O. Donde el I2O sí beneficia a los sistemas es que ayuda al procesador central de la computadora con parte de la carga de trabajo, lo cual le permite ocuparse de otras tareas.

Supervisión del estado del servidor

Una característica importante de la mayoría de los servidores es la capacidad de supervisar sus propios componentes internos y notificar si se está desarrollando real o aparentemente un problema. Por lo general, los servidores grandes pueden supervisar lo siguiente:

- Funcionamiento adecuado del ventilador
- Voltaje del sistema
- Errores del sistema, aun si son corregidos por la memoria ECC
- Errores en los discos, a pesar de que se corrijan de manera automática
- Temperatura dentro de la cubierta del servidor
- Problemas con el sistema operativo
- Apertura de la cubierta de la computadora

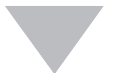
Cualquiera de estos errores podría indicar un problema actual o potencial en el servidor. Por ejemplo, un error de un bit en la memoria que sea corregido por la memoria ECC del sistema no provocará ningún problema al servidor ya que se corrigió, pero podría indicar que un chip de la RAM o un banco de RAM ha comenzado a tener problemas. De manera similar, el incremento de temperatura dentro de la cubierta del servidor no provocaría un problema inmediato, pero podría indicar que un ventilador no funciona adecuadamente, que tiene una toma de aire bloqueada o

que experimenta otro tipo de problema y, al final, la presencia de temperaturas más elevadas que las permitidas por el diseño del servidor provocará alguna falla.

Las soluciones de la supervisión del estado del servidor pueden alertarlo sobre los problemas a través de un correo electrónico o un pager, a fin de que los pueda resolver. Incluso, algunos servidores trabajan si la alimentación del servidor falla o si falla en el cuarto del servidor (a esto se le llama capacidad de "luces apagadas"). Muchos servidores grandes también ofrecen garantías de "prefalla" que establecen que el fabricante deberá reemplazar cualquier componente que reporte aun fallas menores, a fin de que usted los pueda reemplazar antes de que se presente un problema serio. En los servidores de los que dependa y que deben ser lo más confiable posible, dichas características de supervisión y de garantía pueden representar una salvación para su trabajo.

Componentes intercambiables

En estos días, la mayoría de los servidores incluyen componentes intercambiables que usted puede reemplazar mientras el sistema está en funcionamiento. En general, los componentes intercambiables se limitan a los discos, fuentes de alimentación y ventiladores, todos los cuales operan con una configuración redundante. Por ejemplo, un sistema puede tener dos fuentes de alimentación: si una falla, el sistema aún trabaja normalmente y puede reemplazar la fuente de alimentación que falla sin tener que apagar el servidor. De manera similar, la mayoría de las configuraciones de disco RAID le permiten reemplazar un controlador que falla sin tener que apagar el servidor, siempre y cuando los discos estén instalados en un configuración intercambiable.



PISTA Muchos sistemas de disco RAID le permiten instalar un disco de reserva que el sistema utiliza como reemplazo automático de cualquier controlador que llegara a fallar. Por supuesto, usted debe reemplazar el disco que falla tan pronto como fuera posible, y éste se convertiría en el disco de reserva del arreglo.

SELECCIÓN DE SERVIDORES PARA WINDOWS Y NETWARE

En esta sección usted aprenderá acerca de los fundamentos para definir las necesidades del servidor así como para seleccionar y comprar uno de ellos.

Definición de las necesidades

Antes de buscar diferentes modelos de servidor, usted necesita comprender de manera clara las necesidades que el aparato debe satisfacer. De otro modo, se estará arriesgando a comprar de más o de menos, lo cual puede provocarle problemas e incluso llevarlo a gastar más dinero del necesario. Comprar de menos lo obligará a realizar compras adicionales no planeadas, las cuales podrían incluir agregar más discos o más dinero, o aun más: tener que reemplazar el servidor muy pronto. Comprar de más significa que gastó más de lo necesario por un servidor, lo cual puede conducir a su compañía a rechazar su solicitud de compra de un servidor particular. En lugar de hacer esas cosas, usted necesita encontrar el "punto medio" a fin de especificar exactamente el servidor que satisfaga sus necesidades; luego, podrá justificar la configuración requerida del servidor y su costo. Usted no podrá hacer nada de lo anterior, a menos que tenga definidas sus necesidades de una manera clara.

Para especificar las necesidades de un servidor, debe responder las preguntas siguientes:

- *¿Cuál es la vida útil del servidor?* ¿Cuánto tiempo espera usted utilizar el servidor? ¿Lo reemplazará en dos, tres o cuatro años? (La mayoría de los servidores se utilizan alrededor de tres años antes de reemplazarse). Todos deben coincidir en este periodo debido a que si planea reemplazar el servidor en dos años, no tendrá problemas con un servidor más pequeño que si hubiera planeado reemplazarlo en tres o cuatro años. Sin embargo, si usted especificara un servidor capaz de satisfacer las necesidades de aquí a dos años, no querrá llegar al final de esos dos años para darse cuenta de que su compañía no aprobará el reemplazo.
- *¿Qué trabajo llevará a cabo el servidor?* ¿Será un servidor de impresión y de archivos, un servidor web, un servidor de base de datos o algún otro tipo?
- *¿Cuántos usuarios tendrá que soportar el servidor y cuáles son las necesidades de dichos usuarios?* Por ejemplo, si opta por el servidor de impresión y de archivos deberá calcular los requerimientos de almacenamiento y ancho de banda necesarios para satisfacer todas las solicitudes planeadas de los usuarios. En el caso de un servidor de base de datos, usted deberá conocer con qué rapidez debe responder el servidor a las diferentes operaciones de las bases de datos.
- *¿Cuán confiable deberá ser el servidor?* ¿Cuáles son las consecuencias (costos y efectos) si el servidor sale de servicio por una o más horas, o por un día o dos?
- *¿Compartirá tareas en el servidor?* La compartición es una técnica por medio de la cual múltiples servidores comparten la misma tarea principal. Si uno de ellos falla, el sistema sigue trabajando, aunque a una velocidad más lenta. Una vez que se ha reparado el servidor que fallaba, se lo puede agregar otra vez al conjunto.
- *¿Cuán asegurados contra una pérdida deberán estar los datos en el servidor?* Esto es diferente a la pregunta anterior, ya que usted podrá tener casos en los que el servidor nunca deberá perder datos, aun cuando no represente mayor problema si el servidor deja de funcionar por algunas horas. En dicha situación, podría utilizar una configuración RAID 1 o RAID 10, pero no le importarían mucho, digamos, las fuentes de alimentación redundantes. Usted también podría probar con un esquema de almacenamiento jerárquico de algún tipo, donde los datos se copiaran automáticamente en una cinta o disco óptico en tiempo real, o donde hiciera varios respaldos incrementales de los archivos utilizados cada día.
- *Si el servidor falla, ¿cuáles son sus planes de respaldo?* ¿Planea tener disponible un servidor de repuesto (uno que esté listo para intercambiarse en el momento que se detecte una falla en el servidor) o simplemente dependerá de las capacidades del fabricante del servidor para dar servicio? También, a veces, si un servidor falla, otros servidores podrían satisfacer, de manera temporal, algunas de sus necesidades. Por ejemplo, en una red Windows, si un controlador de dominio falla, usted puede tener otros controladores de dominio para proporcionar la funcionalidad necesaria a la red como un todo. O podría contar con colas de impresión redundantes definidas en otro servidor, listas para entrar en acción en caso de que el servidor de impresión principal llegara a fallar.

- *¿Cómo planea respaldar al servidor?* ¿Planea tener un controlador de cinta en el servidor en sí mismo o respaldarlo en la red con la ayuda de algún otro dispositivo de respaldo de servidor? ¿Piensa realizar respaldos mientras el servidor esté en operación o en la noche cuando nadie lo utilice? Estas son preguntas importantes a las cuales debe responder, ya que si usted instala el dispositivo de respaldo en el servidor también necesitará tener software de respaldo en el servidor. Si planea respaldar un servidor mientras esté en operación, necesitará un sistema de respaldo rápido conectado a su bus rápido de servidor a fin de minimizar el efecto a los usuarios durante el día. Si planea respaldar el servidor a través de la red, necesitará un conexión de red lo suficientemente rápida como para manejar la cantidad total de los datos en el servidor. Piense con mucho cuidado acerca de sus planes de respaldo cuando deba determinar las especificaciones de un servidor.
- *¿Cómo pueden cambiar con el tiempo las demandas que se le imponen al servidor?* ¿Está la compañía contratando agresivamente más empleados como para que el servidor tenga que dar soporte al doble de usuarios en un año a partir de ahora y a cuatro veces el número de usuarios en dos años? Asegúrese de conocer los planes globales de la compañía y pondérelos cuando haga el análisis de las necesidades del servidor. También, aun en compañías donde el número de usuarios permanece relativamente estable, la capacidad de almacenamiento que requiere cada usuario crecerá muy rápido. Una regla es calcular que los requerimientos de almacenamiento actuales se duplican cada 18 meses, si todo lo demás permanece igual. Si usted tiene datos históricos de cuánto espacio de almacenamiento consumen los usuarios, dicha información podría ayudarle a calcular los requerimientos de su sistema de una forma aún más precisa. (¡Y no olvide anticipar cualquier nuevo servicio de red que pudiera incrementar más rápidamente sus necesidades de almacenamiento!).
- *¿Puede el nuevo servidor trabajar con cualquier hardware existente?* Si usted tiene que reutilizar un dispositivo de respaldo de red, por ejemplo, deberá asegurarse de que el nuevo servidor puede soportarlo adecuadamente (y viceversa).
- *¿Cuánto espacio físico tiene usted disponible para instalar el servidor?* ¿Está obligado, por motivos de espacio, a adquirir el servidor más pequeño posible?

Una vez que responda estas preguntas y cualquier otra que pueda presentarse, estará en condiciones de buscar diferentes servidores que satisfagan sus necesidades.

Selección del servidor

Aparte de seleccionar los tipos de equipo que necesita para un servidor, debe recordar los tres requisitos básicos que todas sus compras deben cumplir: compatibilidad, compatibilidad y compatibilidad. Si su sistema operativo de red comienza a desplegar mensajes de error en un servidor, necesitará respuestas rápidas a este tipo de problemas. Si usted mismo construye un servidor comprando una tarjeta madre, un controlador de disco, una tarjeta de video, etc., no va a poder conseguir el soporte necesario, ya sea para el hardware o para cualquier problema de compatibilidad que pueda presentarse con el software. En el caso de los sistemas operativos de red de Novell y Microsoft, asegúrese de que cada parte del servidor —así como de todo el sistema en su conjunto— esté certificada por Novell o Microsoft para sus sistemas operativos de red, respectivamente.

Cuando los sistemas operativos sean Microsoft, consulte la URL siguiente para ver la Lista de Compatibilidad de Hardware (HCL) de esta empresa y estar seguro de que el hardware que desee está certificado:

```
http://www.microsoft.com/whdc/hcl/default.msp
```

Cuando selecciona servidores, a menudo elige primero el fabricante y después el modelo que realmente necesita. Esto se debe a que, si todo lo demás permanece igual, estará más a gusto si todos sus servidores son del mismo fabricante. Administrar servidores de un solo fabricante es mucho más fácil que administrar los de muchos. Será para usted más fácil tener refacciones en existencia que puedan instalarse en todos sus servidores y podrá establecer una mejor relación con el fabricante o con el distribuidor, lo cual representa beneficios adicionales. Por ejemplo, Dell le permite a sus compañías clientes que certifiquen a sus técnicos de casa acerca del hardware de su marca (incluyendo servidores), y después les permite ordenar partes de una manera más directa, sin tener que ir al primer nivel de soporte (el trabajo de la gente del primer nivel de soporte es, básicamente, interceptar las preguntas sencillas que hacen los principiantes), y también proporciona otros beneficios.

Sea conservador en la selección de servidores y marcas. Debe aferrarse a los nombres más conocidos de la industria. Cuando seleccione un servidor, deberá optar por los "principales" por muchas razones, dentro de las que se incluyen las siguientes:

- Tienen organizaciones y prácticas de servicio mucho más establecidas.
- Es muy probable que le ofrezcan soporte de muy alta calidad.
- Debido a que muchas otras redes están basadas en su equipo, sus bases de datos de soporte técnico probablemente ya tengan documentado cualquier problema que pueda encontrar en su equipo y, quizá, cuenten con la solución para su problema.
- También es muy probable que el fabricante del NOS cuente con datos acerca de cualquier problema relacionado con los servidores más conocidos en el mercado.
- Cuentan con una ingeniería mucho más avanzada y es muy probable que sus servidores tengan un desempeño mejor y más confiable.

Éstas son solo las razones principales. Usted debe recordar que hubo un tiempo en el que el mantra en los departamentos de sistemas de información administrativa (MIS) afirmaba: "Nadie ha sido despedido por comprar equipo IBM". Una forma de pensar muy similar tiene sentido cuando se adquieren servidores, no solo porque la compra esté más protegida, sino también porque comprarlos a los fabricantes principales tiene más sentido desde el punto de vista del negocio, por las razones que se mencionan en la lista anterior.

Recuerde estas diferencias generales cuando seleccione un servidor, ya sea NetWare o Windows: primero, mientras que cualquier servidor consume mucha RAM, los de Windows trabajan mejor con más RAM que un servidor equivalente NetWare. Si todo lo demás permanece igual, planee proporcionar a un servidor Windows de 50 a 100% más RAM que a un servidor NetWare. Asimismo, los servidores de bases de datos consumen mucha RAM con bases de datos de cualquier tamaño apreciable (10 GB o más grandes), así que planee utilizar *al menos* 512 MB de RAM. (1 ó 2 GB es lo más lógico para lograr el mejor desempeño posible).

Es importante que recuerde que NetWare 3.*x* y 4.*x* son NOS de un solo procesador, mientras que los servidores de Windows pueden trabajar hasta con 8 ó 32 procesadores. También NetWare 5.*x* puede soportar hasta 32 procesadores. Aun así, para un servidor NetWare, usted probablemente deba emplear el procesador Xeon de Pentium más rápido que pueda encontrar, mientras que Windows Server trabajará muy bien con dos o cuatro procesadores más lentos. Asimismo, recuerde que con los servidores de un solo procesador, NetWare tiende a desempeñarse mejor que Windows Server. De acuerdo con la aplicación real, NetWare puede trabajar de 15 a 30% mejor que Windows Server, incluso si usted agrega más RAM a la configuración Windows Server.

Tanto Windows Server como NetWare pueden implantar ciertos niveles RAID por sí mismos. Sin embargo, para lograr un mejor funcionamiento, debe seleccionar un controlador de disco que pueda evitarle esta molestia al NOS. Los controladores de disco de gran desempeño a menudo también tienen una cantidad significativa de RAM como memoria caché de los datos del disco, y usualmente tienen su propio procesador a fin de ayudar a manejar sus problemas. Además, usted siempre querrá utilizar subsistemas de disco basados en SCSI en un servidor. Una estación de trabajo que corra con Windows se desempeña igualmente bien con SATA que con SCSI, pero un servidor puede aprovechar las características de SCSI a fin de mejorar el desempeño significativamente respecto a las interfases de disco SATA.

Seleccionar la configuración real del disco es una tarea relativamente directa. Usted comienza con la determinación de su requerimiento de espacio planeado y actual, y después debe considerar sus necesidades de desempeño y confiabilidad para seleccionar un nivel RAID particular que tenga sentido. (Vea la sección "Topologías de disco: ¡Es un RAID!" en este capítulo para mayor información). Una vez que sepa estas cosas, usted podrá seleccionar la cantidad de espacio en disco que necesita y asegurarse de que el servidor que desea puede manejar sus necesidades actuales y futuras de espacio en disco. Recuerde este consejo: estará más a gusto si sabe que sus necesidades de disco se acabarán y planea comprar espacio en disco adicional a medida que se presente la necesidad. Ello se debe a que la capacidad de los controladores de disco aumenta muy rápido, mientras que los precios caen muy rápido también. La compra de un controlador de 200 GB dentro de un año, por ejemplo, será mucho más barato que comprar el mismo controlador hoy. Solo asegúrese de que el servidor que seleccione pueda manejar todos los controladores que piensa comprar y después instale esos controladores según se necesiten a fin de ahorrarle dinero a su compañía. En el caso de los servidores NetWare, también recuerde que la cantidad óptima de RAM depende de la cantidad de espacio en disco del servidor, por lo que debe pensar en comprar más RAM cuando agrega cualquier cantidad significativa de espacio en disco. Sin embargo, afortunadamente, la misma regla para los discos se aplica para la RAM: los precios tienden a reducirse en forma de espiral y la RAM del mañana casi seguramente será mucho más barata que la actual.

Si usted planea comprar un servidor para Windows Server o NetWare 5.x, seguramente querrá seleccionar un sistema que acepte procesadores adicionales. De esta forma, si se da cuenta de que el sistema se convierte en un cuello de botella en el nivel procesador, podrá instalar procesadores adicionales a fin de reducir o eliminar dicho obstáculo.

Compra del sistema

Una vez que tome una decisión acerca del servidor que desea, su compra es relativamente directa: vaya de compras y obtenga el mejor precio por el sistema que quiere. Asegúrese de que los proveedores con los que hable ofrezcan el nivel de soporte que necesite, tanto para la asistencia en la selección antes de la venta como para el soporte posventa.



PISTA Recuerde que realmente no es "juego limpio" confiar en la experiencia de un proveedor particular para seleccionar un servidor y contestar cualquier pregunta que usted tenga en la preventa, y después, comprarle el servidor a otro proveedor con un mejor precio. Trate de ser justo en sus negocios. No es conveniente que abuse de esta forma de los proveedores que tienen una gran capacidad para proporcionar soporte; si lo hace, seguramente no estarán disponibles para ayudarlo con algunos problemas que surgen después de la venta o en futuras compras. Esto no quiere decir que usted tenga que pagar mucho más por el hardware con estos proveedores: solo tome en cuenta el nivel de servicio del proveedor cuando evalúe las diferentes cotizaciones y recuerde que el precio no lo es todo.

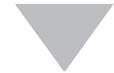
De acuerdo con las prácticas financieras de su compañía, usted puede considerar la opción de rentar un servidor. Hacerlo le puede generar algunos beneficios. Primero, rentar permite a la compañía conservar su efectivo: en lugar de deshacerse de una cantidad de un solo golpe, usted puede pagar por el uso del servidor por un periodo determinado. Asimismo, el efecto anual de una renta es mucho más bajo que una compra y rentarlo podría hacer más fácil escoger un servidor en particular que esté dentro de su presupuesto. Las rentas también tienen un beneficio no visible a primera vista: lo obligan a considerar el reemplazo del servidor al término del periodo de renta (generalmente tres años). En general, las rentas también permiten devolver el servidor a la compañía arrendadora y, después, rentar otro con el que pueda actualizarse. Al final, paga casi lo mismo por rentar que por comprar (considerando todos los aspectos), pero las rentas pueden ayudarle a disciplinar a la compañía a mantener su equipo de cómputo relativamente actualizado. La única desventaja del arrendamiento es que debe tener el tiempo suficiente para reemplazar el servidor al final del periodo de arrendamiento, cuando quizás usted preferiría hacerlo algunos meses antes o después de que éste venza. Aun así, en algunas compañías de arrendamiento los beneficios superan las desventajas. Analice el arrendamiento con su departamento de finanzas antes de ordenar un servidor.

¡Y no invierta mucho dinero en el monitor del servidor! Usted no pasa mucho tiempo frente al monitor (al menos que lo desconfigure) para justificar un monitor de 17 pulgadas para la consola.

Instalación de los servidores

La práctica real de instalar un servidor se refiere de manera específica al servidor en sí y al NOS que planea utilizar. En capítulos subsecuentes se describe la instalación básica de NetWare, Windows y Linux.

Cuando instala un servidor nuevo, recuerde hacer pruebas extensivas del hardware antes de implantarlo. Aunque la mayoría de los servidores son muy confiables cuando son nuevos, el hecho es que si alguna parte va a fallar, casi siempre lo hace al poco tiempo de haberse configurado y puesto a funcionar. Prefiero probar servidores por lo menos una semana, antes de instalar el NOS en el servidor. La mayoría de los servidores vienen con software de diagnóstico que puede configurar para funcionar continuamente, pero debe someter a prueba al procesador del sistema, al subsistema de video, a las superficies de los discos y a la RAM y, además, mantener un registro de cualquier error que se llegase a presentar. Inmediatamente después de sacar el servidor de su caja y antes de instalar cualquier componente que necesite instalar, ponga al servidor en un loop de diagnóstico mediante el empleo de su software de diagnóstico y déjelo correr esas pruebas por el mayor tiempo posible. En ningún caso debe poner a prueba el servidor por un periodo menor a algunos días (trate de ponerlo a prueba por una semana).

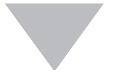


PISTA Es importante que comience a probar el servidor inmediatamente después de recibirlo. La mayoría de los proveedores tienen diferentes políticas de reemplazo contra reparación, en función de cuánto tiempo usted ha tenido el hardware en su poder. Por ejemplo, muchos proveedores reemplazan un servidor por uno completamente nuevo si se descubre una falla dentro de los primeros 30 días, pero después de ese periodo seguirán el procedimiento normal de reparación. Si se presentara un error durante la prueba, usted probablemente se sentirá más a gusto con un nuevo servidor que esperando a que su servidor pase el proceso de reparación. (Además, el proceso de reparación tomará más tiempo).

Después de terminar las pruebas, usted puede instalar el NOS. Durante esta fase, ponga especial atención a cualquier peculiaridad del servidor y a cualquier mensaje de error que reporte el NOS o el servidor durante el proceso de instalación. Usted deberá resolver todos estos errores antes de trabajar con el servidor. En particular, vigile cualquier mensaje intermitente, como un mensaje que indique que existe un error de paridad en la RAM del sistema o un bloqueo inesperado del servidor durante la instalación. Incluso si estos problemas no son recurrentes, consulte con el fabricante del servidor y pida consejos acerca del problema. (Asegúrese de que haya escrito cualquier mensaje u otras cosas que haya notado si esto sucede). Los servidores tienden a fallar en los momentos más inoportunos, así que asegúrese de que se siente totalmente a gusto con el servidor antes de ponerlo a disposición de los usuarios. También tendría sentido dejar el servidor correr su configuración de software por varios días como una prueba adicional antes de ponerlo en servicio.

Asegúrese especialmente de que cuente con todos los NLM (módulos cargables de NetWare) potenciales, los servicios y procesos de Windows o los daemons de UNIX/Linux corriendo como parte de la prueba. Cuando usted combina software de una tercera instancia para estas plataformas, existen muchas probabilidades de que se presenten pequeños errores e incompatibilidades que los proveedores no le notifican al cliente (a pesar del sello de aprobación del NOS por parte del proveedor).

La mayoría de los fabricantes de servidores facilitan la instalación de sus servidores y el NOS en el servidor. Compañías como Compaq empacan sus servidores con CD-ROM especiales que, en su mayoría, automatizan el proceso de instalación de varios NOS en el servidor y también instalan cualquier archivo de soporte necesario que el NOS necesite para trabajar de manera óptima con el hardware del servidor. Antes de instalar un NOS en un servidor, asegúrese de leer cuidadosamente la documentación de éste y aprovechar cualquier herramienta automática proporcionada por el fabricante del sistema.



PISTA El grupo más importante de fabricantes (IBM, Hewlett-Packard y Dell, por ejemplo) mantienen sistemas de notificación de correo electrónico que le permiten saber acerca de los nuevos parches que liberan o cualquier problema serio que presente un modelo en particular. Estos servicios de correo electrónico son extremadamente útiles, por lo que deberá hacer planes para inscribirse con ellos inmediatamente después de que haya recibido el nuevo servidor.

Aquí hay algo más en qué pensar: a veces los servidores se fabrican y después quedan almacenados en el inventario por algunos meses antes de ser vendidos. Como consecuencia, es posible que el servidor no esté provisto con el software más actualizado. Antes de instalar el servidor, verifique el sitio web del fabricante para obtener cualquier actualización que no esté en su paquete de software y defina si es conveniente instalar esas actualizaciones durante el proceso de implantación del sistema.

MANTENIMIENTO Y REPARACIÓN DE SERVIDORES

Para hacer un buen trabajo de mantenimiento y reparación de servidores, necesita dar ciertos pasos para lograr dos objetivos: disminuir la probabilidad de fallas y aumentar las posibilidades de que pueda resolver rápidamente cualquier falla que se llegara a presentar. Los problemas son inevitables, pero usted puede, en gran medida, reducir la probabilidad de tenerlos y también puede mejorar de manera significativa la probabilidad de resolverlos rápidamente si da ciertos pasos antes de que se le presenten problemas reales.

Para reducir la probabilidad de fallas, asegúrese de seguir todos los consejos proporcionados anteriormente: utilice servidores y componentes confiables y que hayan sido probados. Usted también debe dar los pasos adicionales siguientes:

- Siempre que sea posible, trate de reducir el número de trabajos que deba llevar a cabo el servidor. Aunque instalar un solo servidor que sirva a archivos e impresión, base de datos, correo electrónico y servidor web es ciertamente posible, usted estará más protegido (desde el punto de vista de la confiabilidad total) si divide estas tareas en servidores independientes más pequeños.
- Implante una práctica que consista en revisar a menudo el reporte de errores del servidor. Si el NOS del servidor soporta la notificación de errores (como lo hace un pager), considere la implantación de esta facilidad. Muchas fallas comienzan como mensajes de error que pueden ser los antecedentes de una falla real en unas horas, por lo que ser avisado con antelación podría ayudar a mantener el servidor funcionando o, al menos, permitirle resolver el problema en el menor tiempo posible.
- Si un servidor soporta un software administrativo que supervise el estado del servidor, asegúrese de instalarlo.
- La mayoría de los arreglos RAID que soportan la operación de intercambio de unidades de controladores que fallan también requiere que el NOS tenga un software especial instalado para soportar esta facilidad totalmente. Asegúrese de que haya instalado este software antes de que ocurra una falla.
- El software del NOS está entre los tipos de software que se encuentran libres de errores, pero es una verdad indudable que no existe un software que esté completamente libre de ellos. Con el tiempo, cualquier NOS finalmente fallará. A pesar de que muchos servidores pueden trabajar por un año sin requerir que se reinicien, usted estará más a gusto si implanta una práctica que consista en apagar el servidor periódicamente y volverlo a encender. Esta práctica elimina los pequeños errores transitorios que se puedan acumular y puede finalmente provocar una falla mayor en el servidor, como una fuga en la memoria del NOS. El mejor momento para llevar a cabo dicho reinicio del servidor es cada mes.

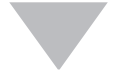
PRECAUCIÓN Asegúrese de hacer un respaldo antes de apagar el servidor y reinicializarlo. La probabilidad más grande de que se presente una falla en el hardware ocurre cuando el sistema se reinicie.

Es una buena práctica realizar tres respaldos y probar los restablecimientos antes de poner en funcionamiento el servidor. Podría parecer redundante, pero uno nunca sabe cuándo necesitará recuperar sus datos y es importante saber que sus prácticas de respaldo y restablecimiento funcionarán adecuadamente.

Usted también puede realizar algunas cosas generales a fin de mejorar su capacidad para resolver rápidamente cualquier falla en el servidor. La más importante es mantener para cada servidor una carpeta extensa (o caja de archivo), que yo llamo un "kit de recuperación". Esta carpeta debe contener lo siguiente:

- Toda la información del servidor que se compró, lo que debe incluir su orden de compra y una copia de la factura del proveedor.

- Un folleto con la configuración del servidor. La mayoría de los programas de configuración de los servidores pueden generar una lista detallada con todos los componentes y sus versiones. En este aspecto, el Insight Manager de HP es excelente.
- Todo el software necesario para reconstruir el servidor completamente desde el inicio. Esto incluye el software de instalación del servidor, el software del NOS, los discos de los controladores de dispositivo y cualquier disco con parches que necesite o haya aplicado. Recuerde agregar a la caja cualquier controlador o parche nuevo que llegue a adquirir durante la vida del servidor a fin de que estén disponibles.
- Obtenga información sobre el servicio del servidor, incluyendo los números de contrato de garantía u otra información que necesite a fin de proporcionarle servicio.
- Una libreta de notas para documentar todos los cambios referentes a la configuración del servidor y cualquier mensaje de error que aparezca. Escriba toda esta información de manera clara, con fecha, hora y cualquier otro detalle que usted (o cualquier otra persona) pueda necesitar para reparar el servidor en caso de que falle.
- Un folleto o documento donde conste cualquier aspecto especial acerca del servidor o de cómo configuró los controladores del disco, incluyendo los parámetros del NOS. Usted necesita estos parámetros en caso de que lo tenga que configurar desde el inicio. Conocer estos parámetros le permitirá recuperar los datos que contienen los discos del servidor de forma que no tenga que recuperar los datos a partir de la cinta de respaldo.



PRECAUCIÓN Usted necesita un fuerte plan de respaldo para cualquier servidor, con las rotaciones adecuadas de cintas y las pruebas regulares de su capacidad para recuperar datos a partir de las cintas que usted haga. El objetivo es no tener que utilizar nunca estas cintas, pero ellas le proporcionarán una red de seguridad absolutamente crítica en caso de que los discos del servidor fallen y pierdan los datos almacenados.

Incluso si es el mejor reparador de computadoras del mundo, deberá trabajar con el departamento de servicio de su fabricante de servidores para reparar cualquier problema. Utilizar este enfoque podría salvarlo ya que el personal de este departamento tiene grandes bases de datos disponibles acerca de los problemas que otras personas han experimentado. También están familiarizados con los pasos a seguir a fin de ayudar a evitar la pérdida de datos a medida que usted trabaja en la reparación del problema. En general, reparar un servidor usted mismo, sin importar qué tanta experiencia y conocimientos posea, es un error.

RESUMEN DEL CAPÍTULO

Cuando instale una red, el primer componente al que deberá poner la mayor atención es al servidor. A pesar de que otras partes de la red, como el cableado, la arquitectura de red o las estaciones de trabajo son también significativas, el servidor es el componente que tiene mayor probabilidad de experimentar un problema. El servidor es el componente en el que deberá invertir la mayor cantidad de tiempo en su administración. Debido a esta circunstancia, sea especialmente cuidadoso en la selección, implantación y mantenimiento de sus servidores. Si cuida su servidor, éste lo cuidará a usted.

El capítulo siguiente trata de las computadoras tipo estación de trabajo de la red y estudia los diferentes requerimientos de las computadoras de escritorio, cómo las debe comprar y administrar y cómo proporcionarles soporte.

CAPÍTULO 14

Compra y administración de computadoras cliente

Las computadoras de escritorio son donde "las ruedas se encuentran con el camino" cuando se habla sobre redes. Estas máquinas son la interfase principal de los usuarios a la red y el recurso del que dependen más para realizar sus trabajos. En realidad, la red está diseñada para facilitar el trabajo de las computadoras de escritorio, y no lo contrario. El mantenimiento de las computadoras de escritorio es también una tarea en la que, a menudo, usted invierte la mayor parte de su tiempo en la administración de la red, por lo que su compra, implantación y administración son importantes. Usted podrá tener la mejor red del mundo, pero si sus computadoras de escritorio no son apropiadas, los usuarios de la red no serán productivos.

Este capítulo se enfoca en la administración de las computadoras de escritorio. Existe la probabilidad de que si usted ha leído este libro, ya conozca los detalles que conforman las computadoras de escritorio y sus sistemas operativos. Usted quizá ya sea un mago en el manejo de Windows y de Macintosh, y se sienta a gusto cuando instala nuevo hardware de computadora y repara problemas en ellas. Si todavía no conoce acerca de estas cosas, existe una buena cantidad de libros que abordan las tecnologías relacionadas con las computadoras de escritorio con más detalle que éste. En este capítulo, la preocupación principal es la forma en que las computadoras se integran a la red y cómo puede aprovecharlas al máximo cuando administre y configure una red.

SELECCIÓN DE LAS COMPUTADORAS DE ESCRITORIO

La selección de las computadoras de escritorio involucra muchas consideraciones. Con el tiempo, hacer una buena elección paga grandes dividendos. Cuando compre computadoras de escritorio nuevas, tendrá la oportunidad de seleccionar máquinas a fin de minimizar el problema del servicio, mejorar la productividad del usuario final, y —sobre todo— conservar el efectivo de su compañía. En las secciones siguientes se analizan los diferentes factores que entran en juego cuando se elige este tipo de computadoras.

Plataformas de escritorio

Usted necesita conocer qué plataforma de cómputo de escritorio va a utilizar. En general, las compañías tienden a dudar cuando escogen entre las tecnologías PC o Macintosh. (En estos días, es muy raro encontrar compañías que dependan en gran medida de las Macintosh como su producto principal en cuanto a computadoras de escritorio). En muy raros casos, dudan entre computadoras de escritorio basadas en Linux o UNIX, pero generalmente tendrá que escoger entre PC y Macintosh.

Cada plataforma tiene sus ventajas y desventajas. Sin tomar en cuenta esta cuestión, usted estará mucho mejor si la compañía pudiera conservar una sola plataforma de cómputo de escritorio como estándar. Las compañías que compraron sus computadoras de escritorio de acuerdo con las preferencias individuales del usuario (por ejemplo, los usuarios son libres de seleccionar PC, Macintosh o alguna otra) terminan con muchos problemas en cuanto al soporte, los cuales surgen a partir de una gran cantidad de fuentes. Proporcionar soporte a dos plataformas de escritorio es dos veces más complejo que a una sola plataforma. ¿Por qué? Considere lo siguiente:



- Usted necesita poseer experiencia en dos plataformas, así como en sus aplicaciones y peculiaridades específicas. En una compañía pequeña, necesita más gente para mantener los niveles de experiencia que se requieren en ambas plataformas que la que necesitaría si tuviera que proporcionar soporte a una sola.
- Requiere mayor existencia de partes de repuesto y hardware de expansión. En general, los componentes que trabajan con una PC no funcionarán en una Macintosh y viceversa.
- Necesita más licencias y más inventario a fin de tener más títulos de software (en promedio, tanto como el doble).
- Los problemas que normalmente no se presentan con una plataforma u otra se presentarán cuando tenga que proporcionar soporte a las dos, aun en la misma red. Proporcionar soporte a dos plataformas es más complejo que hacerlo a solo una, por lo que los servidores deberán correr software adicional, dar cabida a las diferentes formas en las que funcione cada plataforma, etc. Todos estos detalles incrementan la complejidad de la red, lo cual le resta confiabilidad.
- La falta de compatibilidad entre plataformas provoca problemas a los usuarios que tengan que trabajar juntos. A pesar de que utilicen la misma aplicación (como Word, de Microsoft) en PC y Macintosh, las diferencias existen. Por ejemplo, con fuentes de Adobe aun con el mismo nombre se ven y se paginan de manera diferente en Mac y en PC. Los usuarios podrán formatear con muchos trabajos un documento en Word, Excel, FrameMaker y otras aplicaciones disponibles en ambas plataformas solo para darse cuenta que la otra plataforma no presenta su trabajo exactamente de la misma forma. Cuando los usuarios tengan que interactuar entre sí con sus archivos formateados en diversas plataformas, las incompatibilidades se convertirán en un problema muy serio.
- En algunos casos, usted tendrá problemas para encontrar títulos de software con versiones compatibles para ambas plataformas. Esto, en general, significa que los usuarios que utilizan una determinada aplicación no podrán interactuar con los usuarios que utilicen la aplicación funcionalmente equivalente de la otra plataforma. Por ejemplo, Microsoft Access se encuentra disponible solo para Windows, no para la Macintosh. Existen muchos otros ejemplos.
- Usted estará limitado en cuanto a los programas que pueda desarrollar para su uso general. Por ejemplo, trate de desarrollar una aplicación que se base en Microsoft Access y después haga que los usuarios de Macintosh la utilicen. No podrán hacerlo, ya que el programa Microsoft Access no existe en la Macintosh y no hay una forma real de utilizar la misma aplicación de base de datos en ambas plataformas en dichos casos. Usted probablemente podrá intercambiar datos, pero no el programa escrito en Access. La misma situación se presenta en, virtualmente, todos los lenguajes de programación: son casi universalmente específicos para una plataforma, a pesar de los esfuerzos de sus fabricantes de hacerlos neutrales en cuanto a la plataforma en la que se utilicen. Ejemplos de este tipo de problema son mucho más comunes que raros. (Una excepción a esta regla sería una aplicación basada en SQL que hiciera uso de algo como un servidor de base de datos en Oracle, pero este tipo de software no tiene sentido usarlo en aplicaciones sencillas).

Estos ejemplos lo deben convencer de que estará mejor si opera con la plataforma de cómputo de escritorio *equivocada* que con *dos* plataformas de este tipo. Si usted pertenece a una compañía en la que se utilicen dos plataformas, deberá enfocar sus esfuerzos en la implantación de una estándar. Este proceso es difícil y consume mucho tiempo, pero es importante tanto para incrementar la productividad de toda la compañía como para mantener los costos de los sistemas de información (SI) en un nivel razonable. Si instala una red desde el principio, asegúrese de contar con un acuerdo para estandarizarla en una sola plataforma. Asegúrese de que el apoyo para esta estandarización sea aprobada por todos los niveles hasta el presidente de la compañía; de otra forma, la empresa podrá contratar a algún vicepresidente que insista en tener otra plataforma adicional. Si no obtiene este apoyo resuelto con anticipación, podría tener problemas al implantar el estándar.

NOTA Si usted se mueve en el campo de la administración de PC, probablemente se le solicitará llevar a cabo análisis de costos para determinar qué plataforma escoger o justificar por qué la seleccionó. Estos ejercicios incluyen los costos del nuevo hardware y software, tratar con aplicaciones o sistemas tradicionales a la que se tenga que conectar la plataforma y mantener y proporcionar soporte a la misma, así como predecir la factibilidad de la plataforma en uno, dos, cinco y diez años. Recuerde que el director de finanzas es generalmente el jefe del CTO o CIO, ya que los departamentos de IT/IS han sido considerados históricamente un centro de costos más que un centro del cual la compañía obtenga ganancias.

Después de decidir si debe o no estandarizar a una sola plataforma, la decisión que sigue es cuál escoger. Muy a menudo, la compañía tiene una historia con una plataforma en particular, por lo que aferrarse a esa es, en general, la solución más sencilla, a menos de que exista una buena razón para cambiar. Si tiene la fortuna de instalar la red de la compañía por primera vez, entonces podrá ayudar en la selección de la plataforma. Siempre, esta selección deberá ser dictada por lo que los usuarios quieran llevar a cabo, qué aplicaciones necesitan correr y qué plataforma soporta de mejor manera esas aplicaciones. Usted necesita considerar todo el rango de aplicaciones que sea probable que la compañía necesite, pero las necesidades de los usuarios deberán ser las que dicten qué opción tomar. Para la mayoría de las compañías, esto significa que deberá inclinarse por las PC como el estándar. Sin embargo, para otras, las Mac son todavía una buena idea. En general, tiene sentido tener Mac en compañías que muestren un fuerte sesgo a lo artístico y a lo gráfico, como una firma de diseño de páginas web, un negocio de diseño gráfico, etcétera.

NOTA Como probablemente ya habrá notado, mucha gente quiere tomar una decisión sobre la plataforma con base en la que le guste más. Muchas personas se llaman a sí mismos "fanáticos de las PC" o "fanáticos de las Mac". Para personas como éstas, el problema llega casi al mismo nivel de importancia que una religión. Dicha lealtad ferviente a una marca nunca deberá influirlo al tomar una decisión inteligente de negocios. Sin embargo, ¡la presencia de dichas opiniones también significa que deberá negociar de manera muy cuidadosa cuando comente los problemas de cada plataforma con los usuarios del sistema!

Si no existe una necesidad que sugiera de manera definitiva una plataforma en particular, entonces, por muchas razones, usted deberá inclinarse por las PC. Éstas máquinas son las más competitivas en cuanto a precio, su uso es el más difundido, atraen a la mayor cantidad de desarrolladores de software y hardware y tiene mucha más infraestructura para proporcionarles soporte. Asimismo, para ciertas categorías importantes de software de aplicación de negocios,

se encuentran disponibles buenas soluciones en esta plataforma, pero no en la Mac. (En algunas otras instancias, aunque la Mac ofrezca soluciones similares, son inferiores a las que están disponibles para PC).



NOTA A pesar de que el objetivo de este libro es ser neutral en cuanto a plataformas, el hecho es que más de 90% de las computadoras de escritorio en red son PC. Mientras que este libro se aplica tanto a Mac como a PC, lo que resta de este capítulo supone un ambiente PC.

Confiabilidad y servicio

Las características más importantes que hay que buscar en cualquier computadora de escritorio es su confiabilidad y, otra característica íntimamente ligada con la anterior, su facilidad para proporcionarles servicio. Diversos estudios han mostrado que el costo real de una computadora de escritorio es un pequeño porcentaje de su costo a lo largo de toda su vida útil, el cual incluye costos de software, de capacitación y de soporte.

Cuando se analiza la confiabilidad, usted necesita observar todo el panorama. La confiabilidad proviene de varias fuentes. Primero, significa que la computadora utiliza componentes probados de alta calidad. Segundo, que dichos componentes están diseñados desde el punto de vista de la ingeniería para trabajar bien en conjunto. Usted podrá hacer un pastel con los mejores ingredientes disponibles en el mercado, pero si su receta no es buena, el pastel que obtenga no será de buena calidad. Lo mismo se aplica a las computadoras. Aun si utiliza los mejores componentes, éstos no siempre trabajarán juntos de manera óptima. Los fabricantes de mayor prestigio prueban todos los componentes que integran sus sistemas y se aseguran de que sean compatibles entre sí. Tercero, confiabilidad también significa que utiliza una combinación de software en la unidad y que, siempre que sea posible, utilizará software certificado en sus computadoras.

La facilidad para proporcionar servicio a las computadoras está íntimamente relacionada con su confiabilidad. La *facilidad de servicio* significa simplemente que trabajar o reparar una determinada computadora es algo relativamente fácil y rápido. Las características que mejoran di-

Nota del autor

Una vez ingresé a una compañía que había comprado clones “sin nombre” para sus computadoras de escritorio. En mi primera semana, instalé cinco nuevas unidades todavía en sus cajas, solo para darme cuenta de que tres de ellas estaban defectuosas desde su arribo (DOA). Esa misma semana, al director de finanzas (CFO) de la compañía, que trabajaba en una importante actividad financiera, se le descompuso su computadora en varias ocasiones (con la consiguiente pérdida de su trabajo en cada ocasión) hasta que, por último, cambié su computadora por una de las nuevas que funcionaban bien. ¿Valió la pena el dinero ahorrado en esas computadoras (aproximadamente 400 dólares por unidad)? ¿Cuál fue el precio que pagó la compañía por todas esas calamidades? La respuesta es simple: mucho más de lo que la compañía ahorró. Inmediatamente cambié la marca de las computadoras de la compañía a una más confiable (¡el CFO estuvo totalmente de acuerdo!) y me deshice de las máquinas existentes tan rápido como me fue posible. La lección es: cuando compre computadoras no pierda los pesos por ahorrarse los centavos.

cha capacidad son cubiertas que no necesiten de alguna herramienta especial para abrirse, componentes internos que se puedan reemplazar de una manera fácil —como discos duros, memoria y tarjetas de video que requieran herramientas sencillas o que no las requieran— y otras, como un sistema básico de entrada salida (BIOS) de fácil actualización en la computadora. La facilidad para proporcionales servicio a las computadoras está también fuertemente influida por los servicios disponibles del fabricante. ¿Está actualizado su fabricante de computadoras, esto es, ofrece los adelantos más reciente para sus máquinas? ¿Su sitio web ofrece un lugar que le permita encontrar la configuración de su computadora con base en su número de serie o en su número ID de servicio? ¿Está disponible la información técnica acerca de sus sistemas o el fabricante tiende a pasar por alto cualquier problema que encuentre? ¿Qué tan rápido puede obtener las refacciones? ¿El fabricante incluye servicio en el sitio por un periodo que reduzca su responsabilidad de apoyo? ¿Cuál es la garantía que se aplica a las computadoras? ¿Es el fabricante lo suficientemente estable y exitoso como para que pueda esperar que pueda prestarle servicio por toda la vida útil de sus computadoras? ¿Qué otros servicios de valor agregado ofrece si se presentaran problemas en sus computadoras?

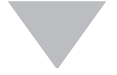
PISTA La revista PC Magazine lleva a cabo un estudio anual acerca de la confiabilidad y la facilidad para proporcionar servicio de los principales fabricantes de computadora e impresoras, con base en las respuestas de miles de sus lectores. Esta información es extremadamente valiosa cuando se debe seleccionar un fabricante y usted deberá prestar mucha atención a los resultados.

A menudo se omiten otros factores que tienen una influencia significativa en la facilidad para proporcionar servicio a las computadoras. ¿Cuántas computadoras vende el fabricante? ¿Es muy usado el modelo específico que desea comprar? Estos factores son importantes porque una computadora que se usa ampliamente en el mercado es muy probable que sea soportada cuando salga nuevo software y hardware. La razón de ello es que las compañías que los hacen saben que deben asegurarse de que sus productos trabajen adecuadamente con esas computadoras. Suponga que usted tiene computadoras de una compañía pequeña local (o, aún peor, usted mismo las construye), y algún paquete de software o sistema operativo que salga en uno o dos años falle en sus computadoras. El fabricante de software o hardware podría decir algo como "Bien, no hemos probado nuestro producto en esa computadora, por lo que no sabemos por qué no funciona bien". A pesar de que el fabricante pueda estar actuando de buena fe para resolver el problema, éste tomará mucho más tiempo para resolverse que si se tratara de un sistema que se usará ampliamente, y puede ser que ni siquiera se resuelva. Por otro lado, si usted utiliza una computadora de una empresa grande, como IBM, Compaq, Dell, HP o Gateway, el proveedor del nuevo producto quizá conozca cómo resolver cualquier problema que se pudiera presentar y lo haya hecho antes de que el producto fuera enviado.

PISTA Si en su compañía se corre una aplicación que es vital para su negocio, pero no es ampliamente utilizada, a veces se justifica investigar qué computadoras utiliza el fabricante de la aplicación. Si usted sabe que el fabricante desarrolló la aplicación utilizando una computadora en particular, puede reducir el riesgo de tener problemas si emplea la misma marca de equipo.

Usted también puede mejorar la facilidad para proporcionar servicio a las computadoras si selecciona un fabricante en particular ya que, entonces, podrá enfocar sus recursos al soporte de esa línea específica de equipo. A las personas de la compañía que proporcionan soporte a

las computadoras de escritorio les será más fácil estar actualizadas con las peculiaridades de ese fabricante y se sentirán más a gusto trabajando. Asimismo, el grupo de soporte de la compañía podrá ser capaz de resolver un problema una sola vez y, después, aplicar la solución a las demás computadoras en lugar de tener que reparar muchos tipos de problemas diferentes en los diversos tipos de computadoras de la compañía. Por último, debe haber beneficios en cuanto a la calidad del servicio cuando usted establece una fuerte relación con un determinado fabricante.



NOTA Si usted proporciona soporte a muchas computadoras, asegúrese de que sean lo más consistentes posibles. No solo debe asegurarse (lo más posible) de que son del mismo modelo y configuración, sino de que el fabricante utiliza los mismos componentes en todas las computadoras de un determinado modelo. Algunos fabricantes no prestan mucha atención a este aspecto; utilizan diferentes modelos de tarjetas madre y de NIC sin registrarlos. Para alguien que solo compra una computadora, esto no representa ningún problema, pero cuando tenga que proporcionar soporte a 500 ó 5 000 computadoras que se supone que son exactamente iguales, pero que no lo son, se convierte en un problema enorme, ya que entonces debe mantener un registro de la información acerca de los diferentes controladores y su configuración. También, si usted instala y proporciona mantenimiento a las computadoras a través del uso de imágenes de disco (como las que fabrica Norton Ghost), tendrá que mantener diferentes imágenes de todos los diferentes submodelos de la computadora.

Precio y desempeño

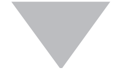
Una vez que se han satisfecho las prioridades anteriores, usted podrá seleccionar el balance adecuado entre desempeño y precio. Para ello necesita tomar en cuenta la vida útil que planee para las nuevas computadoras y asegurarse de comprar sistemas que sean productivos a lo largo de su vida útil. Para determinar este balance, no ponga atención en qué tan bien una configuración en particular maneja las necesidades actuales: enfóquese en qué tan bien manejará las necesidades del futuro.

Algunas personas no estarán de acuerdo con lo que digo, pero creo firmemente que el precio debe ser su *última* prioridad cuando compre computadoras. Aunque el precio de compra es importante, es necesario que usted determine primero sus necesidades y después busque las computadoras que mejor las satisfagan a un precio razonable. Existen diferentes estrategias

¡DEFÍNALO! Vida útil

El término "vida útil" se refiere al tiempo que un activo en particular, como una computadora, podrá desempeñar trabajo útil. La vida útil de una computadora cambiará en función de la marca, el software que necesite para operar, el usuario que la utilice y el presupuesto disponible para actualizarla o reemplazarla. Un programador que necesite el último y más grande hardware y software todo el tiempo, obtendrá una vida útil relativamente corta de una computadora, mientras que una persona que la utilice solo para procesamiento de palabra y correo electrónico y no esté interesado en correr la última versión de software, obtendrá una vida útil mucho más larga. En el caso de la mayoría de las computadoras de escritorio, la vida útil es de 3 a 4 años, aunque es fácil encontrar excepciones a esta regla.

para obtener el mejor precio. Estas estrategias varían desde la oferta directa y la subasta competitiva hasta sacrificar ligeramente la compra desde el punto de vista del desempeño, pero planear mejorar las computadoras existentes cuando sea necesario (al menos en términos de la RAM y el espacio en disco duro, los cuales disminuyen de precio muy rápido a medida que pasa el tiempo).



NOTA No olvide calcular el costo involucrado en el reemplazo o en la actualización de una computadora cuando seleccione un sistema. En general es más barato comprar una computadora más potente que no necesite ser mejorada o reemplazada muy rápido, cuando pondere los costos asociados con la mano de obra y el efecto en la productividad del usuario que resulte de instalar un reemplazo.

Usted puede calcular que las demandas impuestas a una computadora de escritorio se duplicarán cada 24 meses o un tiempo similar, tomando en cuenta su vida útil planeada. Establezca sus niveles de desempeño para satisfacer dicha necesidad. (La gente solía suponer que los requerimientos de desempeño se duplicaban cada 18 meses, pero parece que este lapso se redujo en años recientes). Por ejemplo, suponga que determina que el usuario de hoy requiere un espacio libre en disco de 20 GB, 512 MB de RAM y un procesador Pentium 4 a 1.7 GHz. Es muy probable que en 24 meses sus usuarios estén clamando por 40 GB de espacio en disco, 1 GB de RAM y un procesador Pentium a 44 GHz (o su equivalente). En otros 24 meses (aproximadamente cuatro años a partir de su compra), estas demandas se duplicarán otra vez, a 80 GB de espacio en disco, 2 GB de RAM y el equivalente a un procesador Pentium a 48 GHz. Estas demandas proyectadas podrán parecer poco probables en la actualidad, pero cuando eche un vistazo a las necesidades de hace cuatro años, dichas proyecciones serán bastante razonables.

Utilizando esta manera de calcular las necesidades de desempeño, usted debe ser capaz de encontrar un "justo medio" entre precio, desempeño y vida útil que minimice sus costos y maximice los beneficios que recibirán los usuarios.

REQUERIMIENTOS DE LAS ESTACIONES DE TRABAJO DE LA RED

Las computadoras conectadas a una LAN difieren ligeramente de las computadoras independientes. Las primeras tienen instalado hardware adicional y corren con software de red adicional. Esta sección estudia estas diferencias.

Hardware de las estaciones de trabajo de la red

Todas las computadoras de una red necesitan una interfase de red instalada a fin de conectarse a ella. En general, dicha interfase toma la forma de una tarjeta de interfase de red (NIC), pero algunas computadoras tienen la NIC integrada a la tarjeta madre del sistema. Cada NIC está diseñada específicamente para el tipo de red que soporta. Las NIC están disponibles para las redes Ethernet, Token Ring y otras. En general, las NIC son específicas para el tipo de cable que se haya instalado. Por ejemplo, las NIC de Ethernet se encuentran disponibles para cables 10Base-2, 10Base-T o 100Base-T, pero actualmente están disponibles también la 1000Base-T. Algunas NIC también soportan múltiples tipos de medios de transmisión, lo cual es una bendición si usted se encuentra a la mitad del proceso de migrar de un tipo de medio a otro. Por ejemplo, algunas NIC de Ethernet funcionan con 10Base-2, 10Base-T y 100Base-T en una sola NIC.



Software de las estaciones de trabajo de la red

Las estaciones de trabajo de la red también necesitan software de conectividad para trabajar con ella. Este software consta de varios componentes: un controlador para la NIC, software de controlador para los protocolos que se estén utilizando y un solicitador de red (a menudo llamado *redirector* de la red). Las estaciones de trabajo que actúan en una forma de igual a igual también tienen software de su igual que proporciona servicios de red a otras estaciones de trabajo. Además, podría necesitarse software de servicio de la red, como el que debe utilizar un determinado directorio (por ejemplo, eDirectory de Novell).

Para las computadoras basadas en Windows, usted puede utilizar el software que está incluido para conectarse tanto a redes Novell como a redes basadas en Windows. También puede emplear el software de red de Novell para redes basadas en Novell. Ambos tipos de software trabajan bien aunque existen diferencias entre ellos.

En el caso de las redes basadas en Novell, el software de conectividad de Microsoft consume menos memoria que las de Novell, pero no ofrece tantas facilidades y no se integra muy bien con los servidores de esta marca. Aun así, es confiable y su desempeño es bueno. El software cliente de Novell (llamado Novell Client) trabaja bien y hace un buen uso de las facilidades del servidor Novell y también es más seguro que el software de red de Microsoft.

Cuando utilice el software de Microsoft con el NetWare 4.x o con servidores más grandes, usted debe correr también el software de servicio para acceder al de directorio de Novell. Este software está incluido en Windows y en Novell Client.

Cuando utiliza Windows, usted administra el software de la red por medio de la caja de diálogo Network properties de Network Neighborhood o mediante el objeto Network en el Panel de Control (el cual también accede a la caja de diálogo Network properties). La figura 14-1 muestra un ejemplo de una caja de diálogo.

La caja de diálogo Network properties contiene varias entradas, entre las cuales se incluyen las categorías principales siguientes:

- **Cliente** Usted puede instalar software del cliente en redes Novell o Microsoft. Este software interactúa con los servidores que solicitan servicios de red. En la figura 14-1 puede observar que el Cliente de las redes de Microsoft es un componente instalado.
- **Interfase de red** Esta entrada representa el software del controlador que se instala para cualquier NIC o para los "NIC virtuales" que se utilizan para conectar una red por medio de un módem. En la figura 14-1 puede observar el controlador EtherLink de 3Com listado en los componentes instalados.
- **Protocols** Este software sirve para proporcionar soporte a cualquier protocolo de conectividad de redes que se necesite, como TCP/IP, IPX/SPX o NetBEUI.
- **Servicios** Cualquier software de servicio de red adicional, como el que se utiliza para el DNS también aparece en la caja de diálogo Network properties.

Figura 14-1. Caja de diálogo Network properties en Windows 98.

Usted agrega nuevas entradas ya sean clientes, protocolos o servicios, tecleando el botón Add de la caja de diálogo. Así accede a la caja Select Network Component Type, que se muestra en la figura 14-2. Usted selecciona qué tipo de componente desea instalar y teclea el botón Add.

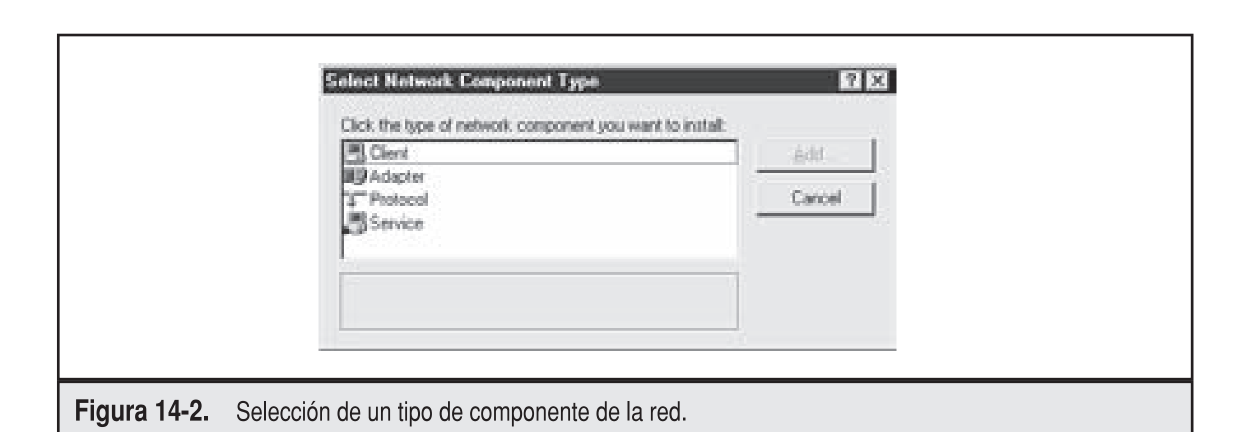


Figura 14-2. Selección de un tipo de componente de la red.

Después de seleccionar qué tipo de componente desea instalar, teclee el botón Add. Enseguida podrá observar la caja de diálogo Select Network Protocol, la cual muestra una lista del software disponible de ese tipo. La figura 14-3 muestra cómo se ve esta caja de diálogo si usted está instalando un protocolo de red adicional. Seleccione el protocolo que desea instalar y, después, teclee el botón OK.

NOTA Cuando utilice el software Cliente de Novell, usará el programa de instalación Cliente de Novell en lugar del anterior. Los resultados aparecerán —y podrán administrarse— en la caja de diálogo Network properties, pero están instalados en forma separada.

Después de seleccionar el software que agregará, regrese a la caja de diálogo Network properties, desde la cual podrá instalar software de red adicional. Después de que haya completado todas las opciones, teclee OK en la caja de diálogo Network properties para guardar los parámetros e instalar en realidad el software en el sistema operativo. El programa le solicita cualquier CD-ROM o diskette que sea necesario para la instalación. Una vez que ésta ha terminado, es necesario que reinicie la computadora a fin de comenzar a utilizar el software. Primero, instale el software del cliente que desee utilizar, ya sea el de las redes Novell o el de las redes Microsoft. Al hacerlo así automáticamente carga los protocolos de los que depende el solicitador, lo cual ahorra tiempo si su red utiliza los protocolos por default.

En la caja de diálogo Network properties, las entradas están *dirigidas* a otras, lo cual les permite trabajar en conjunto. Por ejemplo, los protocolos están dirigidos hacia los NIC, lo que posibilita que el protocolo envíe y reciba ese tipo de paquete. Los clientes son dirigidos hacia los protocolos, lo cual permite que el solicitador de red utilice uno en particular. Por default, esta unión se realiza automáticamente cuando usted instala los componentes. Si existen combinaciones de protocolos o NIC y solicitadores que no utilice, podrá eliminar esas uniones en particular.

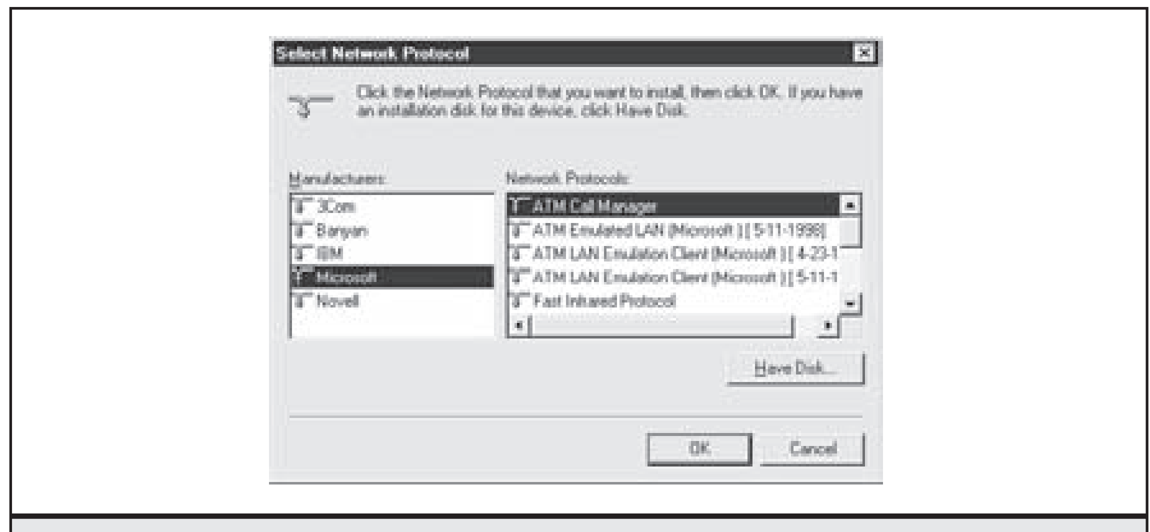


Figura 14-3. Selección de la adición de un protocolo.



PISTA Instale solo los componentes de la red que en realidad necesitará en la caja de diálogo Network properties. Agregar componentes innecesarios como protocolos de conectividad de redes que no se utilicen, reduce innecesariamente el desempeño de la estación de trabajo de la red.

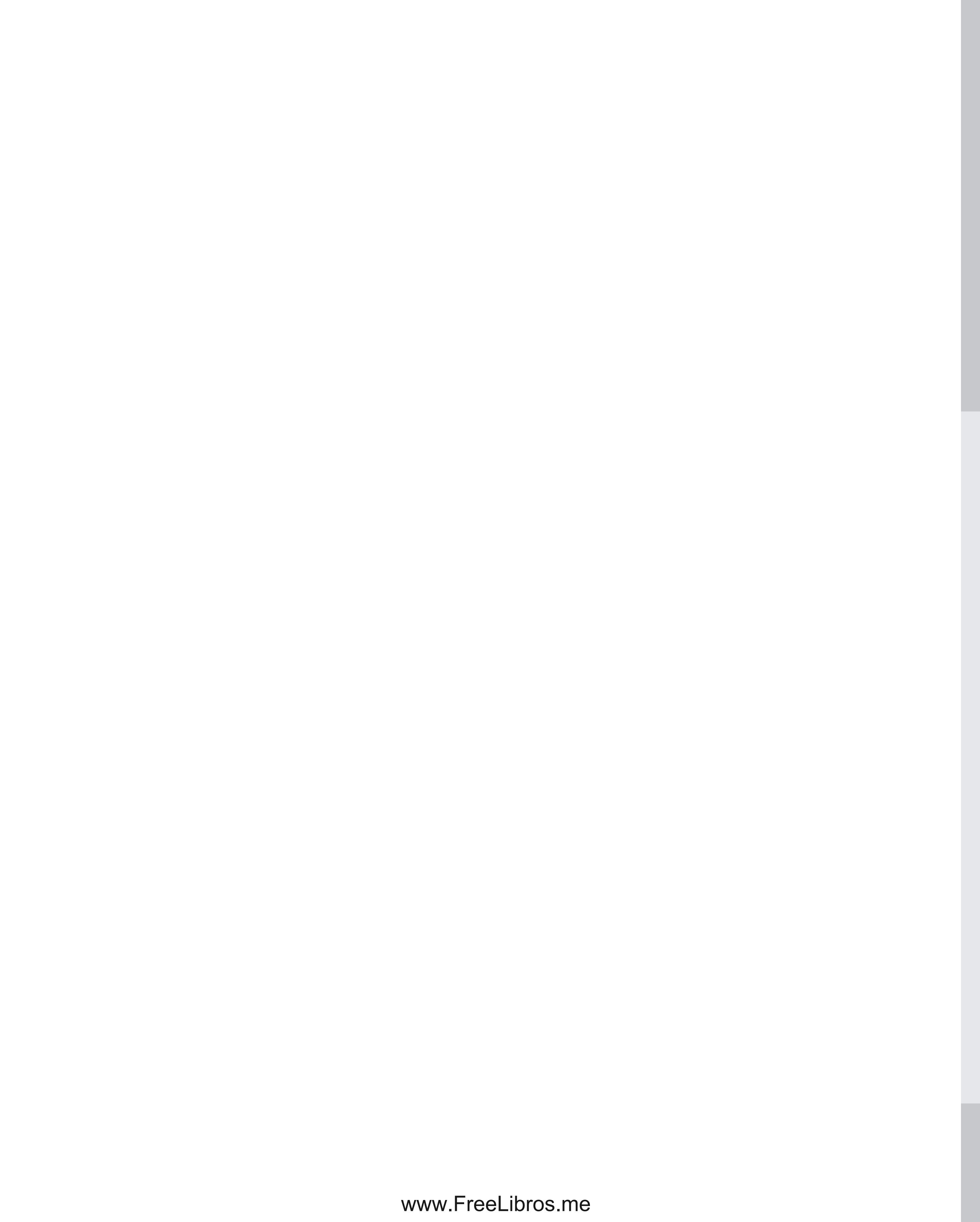
RESUMEN DEL CAPÍTULO

La administración de las estaciones de trabajo de la red puede ser una tarea intimidante. Cada una de ellas debe administrarse en forma diferente, cada usuario puede tener distintas necesidades y, debido a la forma en que se utilizan, las estaciones de trabajo de la red son las que tienen una mayor probabilidad de fallar. En este capítulo usted aprendió información general acerca de las computadoras cliente de la red, junto con la forma de seleccionar las apropiadas. Usted también aprendió acerca de los componentes que las computadoras de red tienen en común, los cuales las hacen diferentes a las computadoras de escritorio independientes.

En el capítulo siguiente aprenderá acerca de los fundamentos de cómo se puede diseñar una red desde el inicio. En general, el proceso de diseño de una red consiste, primero, en comprender a fondo las necesidades que deberá satisfacer dicha red, ponderar con anticipación el crecimiento de la misma y, después, comenzar a delinear cómo estará estructurada y qué tecnologías serán necesarias.

PARTE II

Conocimiento por medio de la práctica



CAPÍTULO 15

Diseño de una red

Los profesionales de la conectividad de redes rara vez tienen la oportunidad de ingresar a una compañía y diseñar una red nueva desde el inicio, pero los que sí han tenido dicha oportunidad son definitivamente muy afortunados. Mientras que dicho esfuerzo involucra largas horas, estrés, fechas de entrega y la preocupación enfadosa de que quizás están olvidando algo, como recompensa, ellos diseñan la forma del ambiente de cómputo de un gran número de usuarios, y —en muchas compañías— definen el nivel de eficiencia con que funcionará en los años venideros. En algunas empresas que dependen de manera muy significativa de las tecnologías de la información, una red que opere de manera eficiente será determinante para el éxito de la compañía. Es una enorme responsabilidad, sin embargo, una de las tareas más gratificantes que usted pueda tener.

Por supuesto, diseñar una red desde el inicio es más la excepción que la regla. En la mayoría de los casos, las redes comienzan pequeñas y, con el tiempo, se desarrollan; son como las células de la piel, pues usted está completamente seguro de que tendrá que reemplazar cada una de ellas dentro de algunos años, pero solo unas cuantas a la vez. Las redes trabajan de la misma manera: crecen a medida que pasa el tiempo, y si las mide ahora y en unos pocos años vuelve a hacer lo mismo, parecería como si se hubiera construido una nueva red. Sin embargo, el proceso es, en general, evolucionario más que revolucionario. Aunque existen excepciones a la regla. Por ejemplo, una compañía se puede cambiar a un nuevo edificio, decidir deshacerse de la vieja red durante el proceso y poner una nueva en su ubicación actual. De la misma manera, una compañía muy sólida que inicie operaciones y que crezca de 5 a 500 empleados en seis meses, es muy probable que contemple la necesidad de una nueva red.

Sin tomar en cuenta si construye una red desde el inicio o renova una ya existente, las herramientas que utilice serán muy parecidas y el proceso de diseño también será semejante. En realidad, el concepto es simple: usted evalúa las necesidades que la red deberá satisfacer y, después, trata de cubrirlas. En la práctica, este proceso es mucho más complejo, pero la idea es muy clara. Aun en una red evolutiva, tiene sentido utilizar la planeación de la red a fin de formular un plan a largo plazo para renovarla. Por tanto, la comprensión de lo que debe analizar cuando construya o renueve una red es muy importante.

El diseño de redes no es, en realidad, una ciencia exacta. Elaborar un diseño *perfectamente* correcto en el primer intento es casi imposible, aun si se cuenta con las mejores herramientas de diseño y recursos disponibles. Esto se debe a que cada red tiene diferentes demandas y éstas, a menudo, interactúan de forma sorprendente. Además, es casi imposible predecir las demandas que deberá satisfacer la red a medida que pase el tiempo, cómo utilizarán los usuarios los recursos de la red y qué otros cambios tendrá que hacer. La situación, en general, es fluida y caótica. La clave está en hacer un buen trabajo en el cálculo de necesidades y, después, hacer el mejor trabajo posible para crear un diseño que las satisfaga. Es también importante contar con planes alternativos, en caso de que alguna parte de la red no trabaje como se había planeado. Por ejemplo, una vez que la red está en servicio y trabaja correctamente, podría darse cuenta de que la distribución del ancho de banda en todos los segmentos es muy pobre. Usted deberá saber con anticipación cómo puede medir y resolver este tipo de problemas. Asimismo, querrá saber si los requerimientos de almacenamiento son mayores o menores de lo que usted esperaba. Es necesario que sepa qué hacer en caso de que esto suceda. El punto es: el diseño de una red es un proceso a menudo interactivo. Su trabajo como diseñador de la red es acercarse lo más posible al diseño que se necesita y, después, hacer los ajustes necesarios.

Gran parte del proceso de diseño de redes estriba en qué tan profundo lo quiera hacer. Existen procesos que son simples, así como también hay otros horriblemente complejos que involucran a docenas de personas, modelado estadístico muy complejo e incluso software de simulación de redes a fin de probar un diseño planeado y ver si trabaja bien. En este capítulo, aprenderá un proceso de relativamente gran alcance que es muy directo y simple. Si utiliza la información de este capítulo, junto con una buena dosis de experiencia, obtendrá una red flexible que satisfará fácilmente las necesidades de cientos de usuarios.



PISTA Usted no puede diseñar una red de cualquier tamaño sin que posea mucha experiencia en trabajos con redes similares; puede administrar todo el proceso si comprende la metodología, pero no podrá elaborar un buen diseño sino cuenta con experiencia. Si es nuevo en el campo de la conectividad de redes y tiene que diseñar una, asegúrese de contar con gente con mucha experiencia en su equipo —ya sea como consultores o como parte de un grupo encabezado por un proveedor— y escuche con mucho cuidado sus conocimientos y experiencia. Escuchar cuidadosamente da como resultado un diseño que trabaje, más que uno que se pueda ver bien en el papel, pero que no sirva para su uso real.

Este capítulo se basa en toda la información que usted recibió en los capítulos anteriores. Piense en este capítulo como el que reúne de una manera coherente toda la información que ya ha aprendido. Los capítulos anteriores se han enfocado en los detalles de las redes, mientras que éste se considera como una vista desde una altura de 30 000 pies donde comenzará a observar cómo trabajan todas las piezas en conjunto.

EVALUACIÓN DE LAS NECESIDADES DE LA RED

La importancia de realizar un buen trabajo cuando se evalúan las necesidades que una red debe satisfacer no puede pasarse por alto. Existen muchos refranes en relación con la importancia de conocer sus objetivos: "Si mides dos veces, solo tendrás que cortar una sola vez" es uno que lo utilizan los carpinteros. "Preparen, fuego, listos" es uno con el que se burlan de la gente que no establece sus objetivos adecuadamente. Y existe un centenar de refranes más. El punto es éste: antes de preocuparse de la topología de red que se debe utilizar, qué plataforma de NOS usar, cómo estructurar sus hubs, puentes y ruteadores y qué grado de cableado instalar, usted necesita conocer los objetivos que debe alcanzar su red. Hacer un buen trabajo puede ser tedioso, pero en la evaluación de las necesidades es donde debe poner el mayor interés durante el proceso de diseño. No hacerlo de manera correcta seguramente traerá como resultado una red improductiva para sus usuarios.



NOTA Muchos profesionales en el área de sistemas de información (SI) son tecnólogos de corazón que adoran jugar con lo último en tecnología. Sea muy cuidadoso para no caer en la tentación de diseñar la red con lo último en tecnología y, después, tratar de investigar de qué manera satisfacen sus necesidades. (Mucha gente, erróneamente, trata de hacerlo así). En lugar de hacer lo anterior, comience con las necesidades y luego investigue qué tecnologías proporcionan soporte para ellas.

Cuando evalúe las necesidades, usted debe encontrar respuestas detalladas a las preguntas siguientes:

- ¿Cuánto espacio de almacenamiento se requiere?
- ¿Cuánto ancho de banda se necesita?
- ¿Qué servicios de red se requieren?
- ¿Cuál es el presupuesto asignado para el proyecto?

Es relativamente sencillo responder estas preguntas básicas como un todo, pero usted necesita analizarlas con más detalle a fin de asegurarse de que no existen agujeros en el diseño de la red que puedan ocasionar problemas. Por ejemplo, sería muy sencillo determinar que la red debe ser capaz de soportar hasta 100 Mbps de ancho de banda, pero necesita saber cómo y cuándo se va a utilizar ese ancho de banda. Si, por ejemplo, el departamento de contabilidad utiliza 90% del ancho de banda cuando se comunica con el servidor, entonces deberá colocar el servidor del sistema de contabilidad y a sus usuarios en su propio segmento de red. Usted no se dará cuenta de dichos problemas y ni cómo atacarlos a menos que su evaluación lo lleve a determinar con cierto grado de detalle cómo se utilizarán los recursos de la red.

Las secciones siguientes estudian qué debe examinar a medida que usted aprende qué debe ser capaz de hacer una determinada red. No existe un orden en particular en el que deban examinarse estos problemas y se dará cuenta de que deberá repasar la lista varias veces a fin de obtener un panorama general. También se percatará de que las necesidades particulares de una compañía requieren más o menos análisis en cada categoría. Se necesita sentido común cuando se diseña una red. Las siguientes sugerencias son reglas generales para iniciarla por la ruta correcta.

Aplicaciones

Un buen punto para comenzar el diseño de una red es enumerar y comprender las aplicaciones que se deberán correr en la red. Finalmente, una red es tan buena como la ayuda que le proporcione a la gente para cumplir con su trabajo y la gente hace su trabajo más directamente por medio del software de aplicación que utiliza. Si las aplicaciones no trabajan correctamente, entonces los usuarios no trabajarán bien, así que la red tendrá que proporcionar un soporte adecuado a las aplicaciones que se hayan planeado.

La mayoría de las redes tienen tanto aplicaciones comunes como específicas a un departamento o a un usuario. Por lo general, la mayoría de las compañías satisface las necesidades comunes de la aplicación mediante de un conjunto de aplicaciones de escritorio, como Microsoft Office o Lotus SmartSuite. Lo que sigue es una lista de las aplicaciones que la mayoría de las compañías simplemente instalan a todos sus usuarios, sin importar si las necesitan o no:

- Procesador de palabra
- Hoja de cálculo
- Base de datos
- Presentaciones gráficas
- Correo electrónico

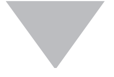
- ■ Administrador de información personal (calendario, lista de contactos, etc.)
- ▲ Software explorador de virus

Su primera orden de negocios es determinar una serie de aspectos acerca de las aplicaciones comunes. Usted necesita conocer si todos los usuarios requieren todas las aplicaciones instaladas, con qué frecuencia planean utilizarlas, cuántos archivos piensan generar y almacenar, de qué tamaño serán dichos archivos y cómo se compartirán entre los usuarios. Por ejemplo, en una población de 1 000 usuarios, usted debe determinar que 90% utilizará procesamiento de palabra para generar un promedio de 10 documentos al mes, y que cada documento tendrá, en promedio, 100 KB, y los usuarios probablemente querrán tener a la mano documentos de por lo menos dos años atrás. Sí, éstos son pronósticos bien informados, pero es importante generar estadísticas razonables. Las experiencias con compañías y poblaciones de usuarios similares pueden ser extremadamente valiosas para elaborar estos cálculos. Solo con esta información usted sabrá inmediatamente que necesita aproximadamente 24 MB de almacenamiento por usuario o 21.6 GB para la población de 900 usuarios que utilizan el procesamiento de palabra, solo para confeccionar documentos hechos con un procesador de palabra. Con frecuencia, en aplicaciones donde los usuarios comparten archivos, usted deberá ponderar que la mayoría de ellos conservan copias personales de algunos archivos que también comparten con los demás.



PISTA Usted puede ayudar a reducir las necesidades de almacenamiento de la red si instala directorios compartidos en los que diferentes grupos de personas puedan almacenar y acceder a archivos compartidos.

Después, haga los mismos cálculos con otras aplicaciones tomando en cuenta sus requerimientos esperados en cuanto a tamaño, frecuencia de creación y almacenamiento a largo plazo.



PISTA No se vaya a quedar empantanado en la "parálisis analítica", preocupándose de si puede demostrar científicamente si sus cálculos son precisos o no. En lugar de hacer esto, asegúrese de que dichos cálculos les parezcan razonables a los demás profesionales involucrados en las redes. En cierto punto del proceso, usted necesitará justificar el diseño y el costo de la red y, para hacerlo, es necesario contar con cálculos razonables. Solo evite sobredimensionar este aspecto.

Después de determinar las aplicaciones comunes, proceda a determinar las aplicaciones específicas de cada departamento. Este paso es un poco azaroso en las redes de compañías nuevas ya que es posible que no conozca qué aplicaciones se utilizarán. En las compañías ya establecidas usted tiene la ventaja de conocer a qué aplicaciones departamentales necesita proporcionarles soporte. Las diferentes aplicaciones departamentales pueden tener en la red efectos muy variados. Por ejemplo, un sistema de contabilidad diseñado en función de archivos de base de datos compartidos necesita un diseño de red muy diferente que uno que utilice un diseño de base de datos cliente/servidor. El primero depende en mayor medida del desempeño del servidor de archivos y es más probable que sea sensible al ancho de banda que una aplicación cliente/servidor que corra en un servidor dedicado. Si todavía no se ha seleccionado una aplicación departamental, hable con los administradores de ese departamento a fin de obtener los mejores pronósticos y después proceda.

A continuación se presentan aplicaciones departamentales que usted debe considerar:

- Contabilidad
- Distribución y control de inventarios
- Manufactura/MRP
- Tecnología de la información
- Comercio electrónico
- Recursos humanos
- Nómina y administración de existencias
- Publicidad
- Soporte a ventas
- Legal
- Otras aplicaciones concernientes a la línea de negocios específica de la compañía

Para cada una de las aplicaciones departamentales que usted identifique, necesita hacerse ciertas preguntas: ¿Qué capacidad de almacenamiento consumirán? ¿Desde dónde se correrá la aplicación: desde computadoras locales con datos en un servidor o completamente desde un lugar central donde tanto los datos como la aplicación corran en una computadora central? ¿Tendrán sus propios servidores dedicados? ¿Cuánto ancho de banda de la red necesitará la aplicación? ¿Cómo se modificarán todos estos factores a medida que la compañía crezca?

Por último, mientras que quizás usted no los haya incluido formalmente en su plan, considere las aplicaciones específicas que puedan correr. Por ejemplo, quizá pueda estimar que sea muy probable que el personal del grupo de investigación y desarrollo (R&D) de la compañía corra dos o tres aplicaciones desconocidas como parte de sus tareas cotidianas. Si decide que las aplicaciones específicas del usuario tendrán un efecto muy significativo en la red, entonces deberá calcular sus necesidades de la misma manera en que lo hace con los demás tipos de aplicaciones. Si decide que tendrán un mínimo efecto, entonces quizás usted decida incluirlas solo parcialmente o de plano no incluirlas.

Usuarios

Una vez que conozca qué aplicaciones soportará su red, podrá estimar a cuántos usuarios necesita proporcionarles soporte y qué aplicaciones utilizará cada uno. Es probable que el cálculo total de los usuarios sea más fácil ya que la compañía seguramente contará con un plan de negocios o un presupuesto a largo plazo a partir del cual usted podrá realizar estos cálculos. Los cálculos sobre los usuarios deberán ser razonablemente detallados: conocer el número de usuarios en cada departamento de la compañía, así como el número total de ellos.

Usted deberá calcular cuántos usuarios necesitarán apoyo inmediatamente, en uno, en tres y en cinco años. A pesar de que cinco años es un horizonte lejano para utilizarse en un cálculo, es importante conocer esta información durante el proceso de diseño. Diferentes velocidades de crecimiento sugieren diferentes diseños de la red, aun en el momento de la concepción de ésta.

Una compañía que estime que tendrá 100 usuarios inmediatamente, 115 en un año, 130 en tres años y 150 en cinco años necesita un diseño de red diferente al de una compañía que estime que tendrá 100 usuarios inmediatamente, 115 en un año, 300 en tres años y 1 000 en cinco años. En este último caso, usted tendrá que invertir más en un diseño que pueda escalarse más rápido y es probable que invierta mucho más al inicio de la construcción de la red, a pesar de que ésta vaya a tener el mismo número de usuarios en los dos primeros años.

Sin embargo, no es suficiente con conocer el número de usuarios. Usted necesita saber más acerca de los mismos. Tome en cuenta, por lo menos, las preguntas que se presentan a continuación a fin de determinar si cualquiera de los puntos siguientes representa un factor importante por considerar, en relación con los usuarios en general o los subgrupos de usuarios:

- **Requerimientos de ancho de banda** Además del ancho de banda necesario para almacenar y recuperar archivos, enviar y recibir correo electrónico y navegar un tiempo promedio en Internet, ¿los usuarios requieren de cantidades significativas de ancho de banda? Por ejemplo, ¿bajarán los científicos una copia del genoma humano una vez por semana? ¿Necesitarán los grupos de usuarios intercambiar grandes cantidades de datos entre sitios diferentes? ¿Correrán software de videoconferencia a través de su LAN y su conexión WAN/Internet? ¿Cuánto tiempo supone que los usuarios de la red navegarán? ¿Enviarán gran cantidad de anexos con mucha frecuencia a través del correo electrónico de Internet?

- **Requerimientos de almacenamiento** ¿Necesitará algún grupo de usuarios un nivel de capacidad de almacenamiento significativamente mayor que el promedio total que usted ya ha determinado? Por ejemplo, ¿el grupo de imágenes electrónicas cataloga millones de documentos en archivos de imágenes en un servidor? Si es así, ¿cuánta gente necesita acceder a estos datos? ¿Necesitará el grupo de contabilidad conservar en línea la información financiera de los últimos diez años? ¿Utilizará o instalará la compañía un sistema ejecutivo de información mediante el cual todos los gerentes puedan consultar los sistemas de contabilidad, distribución y manufactura de la compañía? Y si es así, ¿qué cantidad de ancho de banda adicional o nivel de desempeño del servidor requeriría dicha facilidad?

- **Requerimientos de servicio** ¿Necesitará algún grupo de usuarios servicios de red adicionales que la mayoría de los usuarios no requiere? Por ejemplo, ¿parte de los empleados de la compañía realiza trabajos de tal nivel de sensibilidad que deban ser separados del resto de la LAN por medio de una firewall? ¿Necesitará algún subgrupo de usuarios la facilidad de fax con marcación directa?

Cuando analice los requerimientos de ancho de banda de los usuarios, recuerde poner atención a los momentos en los que se presentan las necesidades de ancho de banda. Si cierto número de actividades conocidas requieren un gran ancho de banda y deben llevarse a cabo durante horas de trabajo normales, pueden afectar el desempeño del resto de la red. Por tanto, asegúrese de calcular las necesidades de ancho de banda promedio y pico.

Servicios de red

A continuación, enfóquese en los servicios que deberá brindar la red, los cuales pueden variar significativamente de compañía a compañía. Una red básica necesitará solo servicios de archivo e impresión, además de la conectividad a Internet, quizás. Una red más compleja necesitará muchos

servicios adicionales. Considere cuáles de los siguientes tipos de servicio, necesita proporcionar la red que usted está diseñando, así como otros que sean específicos de su compañía:

- Servicios de archivo e impresión
- Servicios de respaldo y recuperación
- Navegación a través de la web en Internet
- FTP y Telnet
- Correo electrónico por Internet o externo
- Servicios de seguridad por Internet
- Marcación desde una LAN a través de un grupo de módems
- Marcación hacia una LAN a través de un grupo de módems
- Envío de fax hacia una LAN (distribuido manual o automáticamente)
- Servicios de protocolo de configuración dinámica de host (DHCP)
- Servicios centralizados de protección contra virus
- Servicios WAN a otras locaciones —Envío de señales de radio a través de Internet u otro medio
- Voz sobre IP (VoIP)

Para satisfacer cada servicio debe contestar varias preguntas. Primero, necesita conocer los requerimientos de almacenamiento y ancho de banda de cada servicio y cualquier otro efecto que tenga. Por ejemplo, un servicio de fax requiere, por sí mismo, una pequeña cantidad de espacio de almacenamiento, pero todos los bitmaps de fax que los usuarios almacenarán podrían afectar de manera notable las necesidades de almacenamiento totales. Segundo, usted necesita saber cómo se proporcionará el servicio. Generalmente, esto significa que necesita saber qué servidor proporcionará el servicio. Algunos servicios requieren tan poco espacio que puede asignarlos fácilmente a un servidor que cumpla otras tareas. Un servidor DHCP, que requiere un mínimo de recursos, es un buen ejemplo de dicho servicio. Por otro lado, un sistema de correo electrónico puede necesitar tantos recursos que sea necesario que usted planee asignarlos a un servidor dedicado. Tercero, necesita saber qué usuarios o grupos de éstos necesitan qué servicios. Lo anterior se debe a que, para minimizar el tráfico en la espina dorsal de la red, podría ser necesario dividirla en pequeños segmentos e identificar los servicios que se utilizan con mucha frecuencia por una población de usuarios en particular en el mismo segmento a medida que los utilicen los usuarios.

Seguridad y protección

Todas las consideraciones anteriores están relacionadas con los detalles que requieren las diferentes partes de la red. La protección y seguridad se vinculan con la necesidad de la compañía de mantener la información segura —tanto dentro como fuera de ella— y mantener su información en un lugar seguro para que no sufra pérdidas. Usted necesita estar consciente de la importancia de estos dos aspectos antes de documentar en papel un diseño de red.

Para estas dos cuestiones existe un compromiso entre costo y eficacia. Como se mencionó, ninguna red está totalmente segura y ninguna información está libre de pérdidas. Sin embargo, las compañías y los departamentos tienen diferentes sensibilidades respecto a estos problemas, lo cual indica que se debe invertir más o menos dinero en estas áreas. Algunas aplicaciones son perfectamente adecuadas para almacenarse en un arreglo de discos RAID 0, donde el riesgo de pérdida es elevado (en relación con otros niveles de RAID), pero los datos pueden ser estáticos y fáciles de recuperar a partir de la cinta si el arreglo de discos se pierde. Otras aplicaciones podrían requerir el nivel más alto de seguridad posible contra la pérdida de datos, donde cada servidor tenga arreglos RAID 1 o RAID 10 en espejo y sistemas de respaldo de cinta en línea que actualice una cinta de respaldo cada hora o cada transacción. De manera similar, algunas compañías podrían trabajar con datos tan sensibles que sea necesario instalar las mejores firewalls, quizá dos niveles de éstas y contratar profesionales de tiempo completo dedicados a mantener seguros los datos. Otras compañías se sienten a gusto cuando tienen su información razonablemente segura.

El punto es que usted debe determinar cuál es la importancia de estos aspectos para la compañía para la que diseña la red. Después, puede proponer diferentes soluciones para satisfacer estas necesidades y ponderarlas en el resto de su diseño.

Planeación de la capacidad y el crecimiento

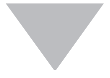
El área final que se debe considerar es el crecimiento esperado de la red, en particular si la compañía espera que este crecimiento sea considerable. Como ya se mencionó, una red diseñada para una compañía de rápido crecimiento se ve diferente de una de crecimiento lento, aun cuando ambas comiencen del mismo tamaño. En el primer caso, debe elaborar un diseño que se pueda expandir rápida y fácilmente sin tener que reemplazar la mayoría del hardware y software existente. En el último caso, usted podrá estar tranquilo con un diseño de red más simple.

También debe considerar el efecto del crecimiento en las diferentes partes de la red que usted ya examinó (aplicaciones, usuarios y servicios), debido a que el crecimiento lineal no siempre significa un efecto lineal correspondiente a la red. Suponiendo un crecimiento lineal, el efecto en la red puede ser mucho más lento, o mucho más rápido que la curva.

Por ejemplo, usted pudo estudiar en el capítulo 4 cómo Ethernet utilizaba un mecanismo de detección de colisiones para administrar el tráfico en la red. En ese capítulo, también aprendió que el escalamiento de Ethernet es lineal, pero solo hasta determinado punto. Una vez que la red comienza a saturarse, el desempeño también comienza a caer rápidamente debido a la naturaleza caótica del esquema de detección de colisiones de Ethernet. Considere una red Ethernet que transmita un tráfico de 3 Mbps. Este tráfico probablemente fluya de manera regular, con solo algunas colisiones y retransmisiones. Sin embargo, si se incrementa la demanda de la red a 4-5 Mbps su desempeño se reducirá hasta detenerse ya que la red se saturará y usted terminará con el mismo número de colisiones y retransmisiones que de datos transmitidos. En realidad, la cantidad de datos válidos que fluye a través de una red Ethernet saturada será menor que la cantidad que fluye a través de una red menos saturada.

Usted puede encontrar ejemplos donde un incremento de la demanda no provoca un aumento correspondiente de la carga en la red y en el servidor. Por ejemplo, la carga en el servidor de un sistema complejo de correo electrónico aumentará solo en una cantidad pequeña si se duplica el número de usuarios ya que los datos de relleno del sistema generan la mayor

parte de la carga. Tampoco los requerimientos de almacenamiento de un sistema de contabilidad se duplicarán solo porque guarde el doble de datos en el mismo; el excedente seguramente consumirá la mayor parte del espacio existente. De forma alternativa, el mismo sistema de contabilidad podrá consumir cuatro veces más espacio de almacenamiento si duplica el almacenamiento de datos, ya que su esquema de indexado es relativamente ineficiente. El punto es que usted necesita saber cómo se escalan las diferentes aplicaciones al aumentar su uso. Los proveedores de las aplicaciones principales que utilice deberán proporcionarle la información necesaria a este respecto.



PISTA Sea cuidadoso no solo al considerar la forma en que las aplicaciones se comportan a medida que se escalan en su ambiente de red. Los diferentes sistemas operativos de red, topologías y computadoras cliente y servidor afectarán la manera en que una aplicación en particular podrá soportar el crecimiento.

SATISFACCIÓN DE LAS NECESIDADES DE LA RED

Una vez que haya terminado su análisis (¡a estas alturas es probable que esté cansado del proceso de evaluación!), podrá comenzar a trabajar en la búsqueda de formas para satisfacer todas las necesidades que haya detectado. Este proceso es en gran medida holístico y no se lleva a cabo mediante una serie de pasos para terminar con una sola respuesta, como una ecuación. En lugar de ello, usted debe comenzar delineando las diferentes partes de la red, considerando los tres puntos principales analizados en esta sección y luego“construir un panorama completo” del diseño de la red. El diseño que usted elabore debe incorporar todo el conocimiento que haya aprehendido durante la evaluación, tomando en cuenta su experiencia y el consejo que consiga para imaginar un diseño concreto que dé por resultado una lista de equipo, una especificación y una configuración.

Es muy importante solicitar críticas de su diseño de otros profesionales que estén involucrados en el campo de las redes, quienes seguramente tendrán experiencias muy valiosas que podrá ponderar. No existe un solo profesional en el campo de las redes que haya visto o haya enfrentado todas las necesidades de diseño posibles, por lo que seguramente usted deseará combinar el consejo de tanta gente con experiencia como le sea posible.

Selección del tipo de red

Usted probablemente desee comenzar el diseño con la selección de un tipo de red. Ésta sería una decisión relativamente muy directa, basada en los requerimientos generales de ancho de banda. En la mayoría de las rede nuevas, casi seguramente usted deberá optar por utilizar una de las versiones de Ethernet que, definitivamente, es el tipo más común de red instalada en la actualidad y es una selección automática muy sencilla.

Usted también necesita decidir qué nivel de Ethernet necesita. Para realizar el cableado hasta el escritorio, usted deberá seleccionar 100Base-T. Es confiable y proporciona mucha capacidad para satisfacer la mayoría de las necesidades. Para la espina dorsal de la red, usted puede utilizar una conexión de alto ancho de banda, como 1000Base-T, sin incurrir en gastos adicionales significativos.

Selección de la estructura de la red

A continuación debe decidir cómo planeará la estructura de la red. En otras palabras, ¿cómo arreglará y cableará los hubs, switches y ruteadores que su red necesita? Ésta quizá sea la cuestión más compleja de resolver, debido a que es difícil predecir qué cantidad de datos debe fluir de un conjunto de nodos determinado a otro. Aun así, usted debe realizar cálculos, basados en el trabajo de evaluación, que le ayudarán a tener un panorama más claro. Si pudiera identificar patrones de alto tráfico que se esperan tener en la red, podría también dibujar un esquema de la red que indicara estos patrones a fin de mejorar la estructura de la red. Recuerde los consejos siguientes:

- El manejo de colisiones de CSMA/CD de Ethernet significa que la red Ethernet trabajará aproximadamente a un tercio de su velocidad nominal. En otras palabras, un segmento 10Base-T, que tenga una velocidad de 10 Mbps, en la práctica trabajará aproximadamente a 3.3 Mbps. Lo mismo para el 100Base-T, que trabajará a una velocidad de datos de 33 Mbps aproximadamente antes de que su desempeño comience a degradarse.
- Siempre que le sea posible, utilice cableado "dirigido hacia un solo sitio" de todos los nodos, hacia un solo closet de cableado o al cuarto del servidor. (El cableado "dirigido hacia un solo sitio" significa que cada cable de red corre desde cada estación de trabajo hasta un solo punto específico). Seguir este procedimiento le permitirá cambiar la estructura de la red de una manera fácil (por ejemplo, dividir los segmentos en otros más pequeños) a medida que cambien las necesidades.
- Excepto en las redes más pequeñas, planee tener un bus principal en la red al cual se conecten. Un switch de Ethernet, más que un hub no conmutado, deberá administrar el bus principal, por lo que cada hub constituye un solo segmento o dominio de colisiones. Con todo, usted deberá tratar de conservar el tráfico en cada segmento por debajo del punto de saturación, pero esta estructura le proporcionará una gran flexibilidad para alcanzar esta meta.
- En estos días, el costo de los switches de Ethernet ha disminuido lo suficiente como para que usted los utilice como hubs. No es del todo exagerado emplear el hardware actual para cablear todo con 100Base-T utilizando solo switches, y no es más caro que utilizar una combinación de hubs y switches.
- La forma del edificio le dictará cómo deberá estructurar la red. Por ejemplo, un edificio mayor a 200 metros en cualquier dimensión probablemente no podrá emplear un esquema de cableado dirigido hacia un sitio en todos los nodos. Ello se debe a que la red Ethernet por par trenzado generalmente tiene un alcance de 100 metros, lo cual incluye el enrutamiento alrededor de los obstáculos que puedan presentarse en el edificio, los cables de parcheo y otras cosas que hagan que la distancia real que cubra el cable sea mayor que la que usted pueda medir sobre el plano del edificio.
- En edificios con múltiples pisos que sean demasiado grandes para un esquema de cableado dirigido hacia un sitio, considere instalar el bus principal en forma vertical de piso a piso y, después, contar con closet de cableado en cada piso, en los cuales se encuentren instalados los hubs para dar servicio a los nodos de ese piso en particular.

El cableado desde el closet de cada piso estará dirigido a cada nodo ubicado en ese piso.

- Considere que la velocidad de bus principal será 10 veces la velocidad de la red hub/escritorio. Si usted utiliza hubs 10Base-T para conectarse con las computadoras de escritorio, planee instalar un bus principal 100Base-T. Si utiliza 100Base-T hacia el escritorio, considere una conexión de red del orden de gigabits como 1 000Base-T para el bus principal.
- La mayor parte del tiempo, muchos nodos llevan a cabo la mayoría de sus comunicaciones a uno o dos servidores de la red. Si usted desea tener servidores específicos para cada departamento o si puede identificar patrones similares, asegúrese de que cada servidor se encuentre ubicado en el mismo segmento en el que estén los nodos a los que prestará servicio.
- Si sus servidores tienden a no estar asignados o a prestar soporte a los departamentos en lugar de proporcionarlo a toda la compañía, asegúrese de que los servidores se encuentren directamente conectados al switch Ethernet del bus principal.
- Si usted cuenta con cualquier número de usuarios que consumen un gran ancho de banda, considere conservarlos en un segmento independiente del resto de la red (si es posible) así como aumentar la velocidad de ese segmento a 100 Mbps o 1 000 Mbps, si fuera necesario.
- A medida que comience a implantar la red, observe con mucha atención la relación entre los paquetes en colisión y los paquetes de datos. Si el número de colisiones en cualquier segmento se eleva a 5 ó 7% del número total de paquetes, el desempeño de la red comenzará a degradarse; usted necesita investigar la causa y buscar una forma de disminuir este cociente. En general, logrará este objetivo si divide el segmento en pequeñas porciones o configura los switches en una LAN virtual o VLAN, a menos de que conozca otra forma de reducir la cantidad de tráfico.

Selección de los servidores

Cuando seleccione los servidores de una red, comience por determinar qué sistema operativo de red utilizará. En el caso de las redes centradas en PC, la decisión está generalmente entre NetWare 5 de Novell y Windows 2000 Server. Siempre que sea posible, evite utilizar ambos, ya que proporcionar soporte a dos sistemas de NOS hace que la administración de los servidores sea mucho más difícil. Usted se sentirá más a gusto comprometiéndose con una sola plataforma NOS que tratar de tener ambas.

Después, haga una lista de los diferentes servicios de red que sus servidores deban proporcionar. Su objetivo debe ser encontrar formas diferentes para tener en sus servidores estos servicios, pero deberá hacer un balance entre una serie de factores:

- Si todo lo demás permanece igual, utilizar más servidores pequeños para almacenar un menor número de servicios en cada uno es más confiable que utilizar un número menor de servidores grandes para almacenar muchos servicios.

- De lo contrario, contar con más servidores pequeños aumenta la probabilidad de que un servidor falle en cualquier momento.
- Utilizar una mayor cantidad de servidores pequeños es más caro y requiere más mantenimiento que utilizar una menor cantidad de servidores con mayor capacidad.
- Si usted piensa utilizar más de un servidor, considere qué servicios deberán tener redundancia en otro y cómo planea atacar las fallas que se presenten en cualquier servidor.

Con base en la información que arrojó su evaluación, usted podrá determinar fácilmente qué capacidad de almacenamiento necesitarán sus servidores. Sin embargo, es más difícil determinar la capacidad de cada servidor en términos de potencia del procesador, RAM instalada y otras características, como la configuración del bus. Para satisfacer estas especificaciones, será necesario que usted confíe en el consejo del proveedor del NOS y del fabricante de los servidores. Por fortuna, tanto Microsoft como Novell han publicado pruebas y recomendaciones respecto al tamaño de los servidores dados los diferentes servicios y cargas de usuario. Muchos fabricantes de servidores de primer nivel también cuentan con dicha información a fin de ayudarle a seleccionar un modelo de servidor y sus especificaciones.

RESUMEN DEL CAPÍTULO

El proceso de diseño de una red puede ser extremadamente complejo. Aun si se dedicara un libro completo a esta cuestión, no existe una forma de abordar este tema con la suficiente profundidad para convertirlo en poco tiempo en un experto en el diseño de redes. Si usted se encuentra en la envidiable posición de tener que diseñar una red, sería mejor que comenzara con la estructura que se describió en este capítulo y utilizara otros recursos para contestar preguntas específicas. Existen muchos recursos que le ayudarán, los cuales van desde libros dedicados a los diferentes aspectos del diseño de redes, administración de servidores, mejora del desempeño de una red y administración de NOS específicos, hasta consultores con una amplia experiencia en redes similares y los diferentes proveedores con los que usted trabaja en la planeación de sus compras. En realidad, ¡existen tantos recursos que pueden ayudarle a cumplir con esta tarea, que podrá verse en problemas para decidir qué consejo seguir!

Recuerde siempre dejar algunas válvulas de escape en cualquier diseño de red que realice a fin de que pueda responder de manera rápida a la presencia de nuevos requerimientos o cambio de los mismos, muchos de los cuales se presentarán cuando esté a punto de finalizar el diseño. La buena noticia es que, si usted sigue los consejos de este capítulo y del resto del libro, junto con los demás recursos mencionados, es muy probable que termine por elaborar un diseño de red sólido, que pueda expandirse y mantenerse, y que cumpla con las necesidades de la compañía y del que pueda sentirse orgulloso.

CAPÍTULO 16

Instalación y configuración de Windows 2000 Server

En este capítulo, usted aprenderá cómo instalar Windows 2000 Server. Sin embargo, antes de instalarlo, deberá realizar diversas preverificaciones que preparan el sistema para este proceso. Enseguida, deberá realizar la instalación real, proporcionando la información necesaria que necesite el programa. Por último, deberá probar la instalación solicitando que una computadora cliente acceda al servidor correctamente y lleve a cabo algunas tareas básicas en la red.



PISTA Este capítulo y los dos siguientes ofrecen una introducción general a Windows 2000 Server. Aquí no se describirán ciertos escenarios y técnicas avanzadas de la instalación. Para aprender acerca de otras opciones y características disponibles cuando se instale, administre y utilice Windows 2000 Server, consulte un libro dedicado a este tema, como *Windows 2000: The Complete Reference*, de Kathy Ivens y Kenton Gardinier (McGraw-Hill/Osborne, 2000).

LAS VERSIONES DE WINDOWS 2000

Windows 2000 es una familia completa de productos, todos construidos, en esencia, con el mismo código de programación, pero con diferencias significativas en cuanto a sus características y puesta en marcha. Windows 2000 es una mejora de la línea de productos Windows NT, la cual terminó con Windows NT 4.

La versión de escritorio de la familia de productos se llama *Windows 2000 Professional*, diseñada para correr en computadoras de escritorio en negocios y no es una mejora de Windows 9x/Windows ME. Windows 2000 Professional tiene las características siguientes:

- Corre en sistemas que cuenten con un mínimo de 64 MB de RAM. (Microsoft asegura que Windows 2000 Professional corre más rápido que Windows 9*x*/ME en sistemas con 64 MB de RAM, una afirmación muy impresionante que deberá comprobar por sí mismo).
- Soporta hasta 4 GB de RAM física.
- Soporta uno o dos procesadores.
- Trabaja con Windows 2000 Server para aprovechar las facilidades de Active Directory e Intellimirror.
- Proporciona soporte a dispositivos "conéctese y ya" (PnP, de plug and play). (Windows NT, en realidad, no ofrecía soporte para PnP).
- Incluye todas las facilidades de Windows NT, dentro de las que se encuentran un sistema operativo preferente, protegido y de multiproceso.
- Soporta totalmente facilidades de computación móvil, lo cual incluye la administración de la energía.

La edición estándar de Windows 2000 Server es la versión de servidor principal de Windows 2000. Incluye todo el poder de directorio activo (Active Directory), así como las facilidades siguientes:

- Nuevas herramientas de administración (comparadas con las que proporciona Windows NT) basadas en la Consola de Administración de Microsoft (MMC).
- Servicios de terminal de Windows, que le permiten almacenar aplicaciones gráficas, de forma muy parecida a las aplicaciones hosts de una computadora grande para terminales tontas.
- Servicios de Internet y de la web (DHCP, DNS, servidor de información de Internet y servidor índice).
- Servicios RAS y VPN.
- Servicios de transacciones y mensajería.
- Soporte de hasta cuatro procesadores.
- Soporte de las versiones más recientes de los protocolos estándar de red.

El Servidor Avanzado de Windows 2000 es la oferta de medio alcance de la línea de productos de Windows 2000 Server, que mejora las facilidades de éste pues agrega las siguientes características:

- Proporciona soporte de hasta 8 GB de RAM instalada.
- Balancea la carga de la red. (Por ejemplo, Advanced Server puede compartir una carga significativa de tráfico TCP/IP entre un gran número de servidores y balancear sus cargas).
- Agrupamiento de Windows 2000.
- Proporciona soporte de hasta 8 procesadores.
- Proporciona soporte para 2 nodos.

La versión más poderosa de Windows 2000 Server es la Datacenter Server, la cual es útil cuando es necesario almacenar grandes bases de datos para miles de usuarios o cuando a Windows 2000 Server se le presenta otro tipo de demandas extremadamente pesadas. El Datacenter Server incluye todas las facilidades de otras versiones de Windows 2000 Server, más lo siguiente:

- Proporciona soporte de hasta 64 GB de RAM instalada.
- Proporciona soporte hasta para 32 procesadores.
- Proporciona soporte para grupos de 4 nodos.

PREPARACIÓN DE LA INSTALACIÓN

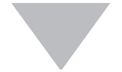
Antes de instalar Windows 2000 Server, usted debe preparar la computadora que se utilizará como servidor y tomar decisiones importantes acerca de la instalación. Esta etapa de preparación consta de un gran número de tareas, incluyendo las siguientes:

- Asegurarse de que el hardware del servidor está certificado para su uso con Windows 2000 Server.
- Verificar que el servidor se encuentre configurado apropiadamente para soportar Windows 2000 Server.
- Llevar a cabo las pruebas de preinstalación necesarias en el hardware del servidor.
- Analizar el hardware antes de llevar a cabo la instalación.
- Decidir cómo va a instalar Windows 2000 Server, después de reunir toda la información acerca de la configuración que usted necesitará durante la instalación.
- Respaldar el sistema antes de llevar a cabo una actualización.

Estas tareas se analizarán en las secciones siguientes.

Verificación de la compatibilidad del hardware

Microsoft mantiene una extensa lista de compatibilidad del hardware (HCL) que muestra los diferentes componentes del hardware y su estatus de prueba sobre varios productos Microsoft, como Windows 2000 Server. Para evitar problemas con su servidor, es importante que se asegure de que éste y cualquier otro periférico instalado hayan sido probados con Windows 2000 Server y que trabajen correctamente. La última versión del HCL puede encontrarse en **http://www.microsoft.com/hcl**. También podrá encontrar una copia basada en texto acerca del CD-ROM Windows 2000 Server. Sin embargo, es preferible utilizar el web HCL, ya que éste podrá tener información más actual que el archivo incluido en la instalación del CD-ROM.



NOTA Si un componente de hardware de su servidor no se encuentra en la HCL, no está todo perdido. Por alguna razón, la HCL puede no tener la información más actual y el hardware que usted desea utilizar puede estar certificado, pero no incluido en la lista todavía. Es mejor verificar con el fabricante del hardware, ya que esa compañía debe conocer el estado actual de su certificación. Asimismo, los productos que no aparecen en la HCL podrían funcionar bien con Windows 2000. Si usted utiliza un servidor para fines de prueba o para soportar servicios limitados y está a gusto con él, puede proceder a instalar Windows 2000 Server y comenzar a trabajar. Sin embargo, no deberá hacer lo anterior en servidores de producción de los que dependan muchas personas. No solo una incompatibilidad pasada por alto puede causar serios problemas con un servidor no certificado, sino que usted no podrá obtener el nivel más alto de soporte de Microsoft para el hardware que no está certificado todavía. Por esta razón, debe evitar la utilización de servidores que todavía no estén certificados por Microsoft.

Verificación de la configuración del hardware

La compra de una computadora para su uso como servidor puede convertirse en una difícil tarea. Usted tendrá que lidiar con una gran cantidad de detalles relacionados con la RAM que desea instalar, la configuración del procesador, la configuración del disco y otras cuestiones por el estilo, así como ponderar la necesidad de realizar una configuración razonable del servidor.



NOTA El capítulo 13 contiene información acerca de las diferentes tecnologías de servidores y la especificación de un servidor de propósito general.

Windows 2000 Server requiere de configuración de hardware *mínima* siguiente:

- Un procesador clase Pentium a 133 MHz o mayor.
- 256 MB de RAM.
- Aproximadamente 1 GB de espacio libre en disco para llevar a cabo la instalación.
- Un CD-ROM o conexión de red desde la cual se pueda instalar Windows 2000 Server. Si usted utiliza un drive de CD-ROM, Microsoft recomienda uno que funcione a una velocidad de 12x o más rápido.

Los requisitos anteriores son los mínimos especificados por Microsoft. Usted deberá considerar utilizar hardware más poderoso del especificado, particularmente para cualquier tipo de servidor (incluso uno que soporte algunos usuarios solamente).

En lugar de lo anterior, siga el siguiente consejo cuando configure un servidor para Windows 2000:

- Comience con al menos un solo procesador Pentium IV rápido que corra a 1 000 MHz o más. Los procesadores Pentium 4 Xeon son muy útiles en un servidor y deberá considerar el precio de esos sistemas en relación con la mejora esperada en cuanto al desempeño. (Si todo lo demás permanece igual, un procesador de la familia Pentium 4 Xeon se desempeñará aproximadamente de 15 a 20% más rápido que un procesador equivalente Pentium 4). Asimismo, considere utilizar un sistema que tenga dos o más procesadores o la facilidad de agregar más después si sus necesidades son mayores de las que esperaba.
- Windows 2000 Server corre mejor en sistemas que tengan una gran capacidad de RAM. En el caso de un servidor, asegúrese de que cuenta al menos con 384 MB de RAM. Si planea proporcionar soporte a los diferentes servicios disponibles en Windows 2000 Server (como Servicios de Terminal, RAS, DHCP, DNS, etc.), entonces 512 MB de RAM podrá ser una mejor opción que 384. Un gigabyte de RAM es una cantidad razonable, en particular, en servidores que trabajen con una gran carga de tráfico. (No olvide que usted puede comenzar con 384 MB e instalar más si fuera necesario y posiblemente a un menor precio que cuando compró el servidor). No intente correr Windows 2000 Server en un sistema con menos de 256 MB.
- Es importante contar con un subsistema de disco basado en SCSI rápido, en particular, en servidores que van a almacenar una gran cantidad de datos. Consulte el capítulo 13 para obtener más información acerca de la selección de sistemas SCSI cuando se utilizan diferentes niveles de RAID y otra información importante del disco.
- Windows 2000 Server requiere una gran cantidad de espacio en disco para su configuración especial. La fórmula para determinar la cantidad de espacio en disco es de 850 MB + (RAM en MB ×2). En otras palabras, usted necesita 850 MB, más otros 2 MB de espacio en disco por cada megabyte de RAM instalado en el servidor, que es la cantidad mínima que se requiere para la instalación. Para instalar el servidor en un sistema que utilice discos formateados FAT 32 (tabla de localización de archivos) se necesitan 150 MB adicionales más o menos, ya que el FAT32 almacena archivos de una forma no tan eficiente como el NTFS. Instalar el Windows 2000 Server a partir de un punto de ins-

talación de red también requiere más espacio en disco: calcule aproximadamente 150 MB de espacio en disco adicional si instalará a partir de una conexión de red en vez de un CD-ROM.

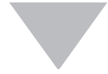
Utilice la información del capítulo 13 que le pueda ayudar a dimensionar su servidor, pero recuerde esta regla: compre el servidor más poderoso que pueda y asegúrese de que tenga la capacidad de expandirse, con el fin de poder satisfacer sus necesidades futuras, por medio de la adición de más memoria RAM, más procesadores y más espacio en disco. A pesar de tomar en cuenta todo lo anterior, es común que los servidores tengan que ser reemplazados de tres a cuatro años a partir de la fecha en la que se pusieron en servicio.

Prueba del hardware del servidor

Usted ya encontró todo el hardware del servidor en el HCL de Windows 2000 Server, ya se aseguró de que su servidor se encuentra perfectamente dimensionado, ya lo compró y cuenta con sus CD-ROM flamantes con el nuevo Windows 2000 Server en el lugar, listos para ser instalados. ¿Ya es hora de comenzar la instalación? Bueno, no precisamente. Antes de que instale cualquier NOS, en particular en un servidor que se utilizará en producción, asegúrese de que ha hecho pruebas (conocida como la prueba de fuego) en el servidor antes de instalar Windows 2000 Server. El hardware de la computadora tiende a ser más confiable después de que ha funcionado por mucho tiempo. En otras palabras, las fallas tienden a presentarse cuando el equipo es nuevo, y la probabilidad de que una falla de hardware se presente disminuye rápidamente después de que ha funcionado de 30 a 90 días. Debido a ello, es una buena idea poner a prueba los servidores nuevos por un periodo de una semana al menos (hacerlo por dos semanas es aún mejor) antes de proceder a instalar el NOS. Tomar esta precaución puede ayudar a que se presente cualquier falla temprana en el equipo durante el tiempo en el que sea fácil de reparar y no afecte a ningún usuario o a la red. Además, la mayor parte de los servidores manejan una política de 30 días para cambio o devolución por parte del fabricante, por lo que si encuentra problemas en el servidor, tendrá la oportunidad de cambiar el sistema y quizá, comenzar con otro modelo.

Usted puede probar el hardware utilizando el software de diagnóstico que viene con el servidor o con el que pone a su disposición el fabricante del mismo. Gran parte del software de diagnóstico le permite seleccionar qué componentes del sistema se desean probar y probarlos en un loop sin fin, lo que hará aparecer cualquier error en un disco flexible o en la pantalla. Usted deberá enfocar las pruebas en los componentes siguientes:

- Procesador(es)
- Componentes de la tarjeta del sistema (controles de interrupción, controladores de acceso directo a memoria [DMA], y otra circuitería de soporte a la tarjeta madre)
- RAM
- Superficies de los discos



PISTA A menudo, el software para la prueba de servidores le permite seleccionar si desea llevar a cabo una prueba destructiva o no destructiva de los discos. (Destructiva significa que cualquier dato que contengan los discos será borrado durante la prueba). La prueba destructiva funciona mejor para descubrir errores en los discos. Ésta es una razón por la que usted querrá llevar a cabo esta prueba antes de instalar el NOS.

Si el software de diagnóstico le permite hacerlo, generalmente podrá excluir, de manera segura, componentes como el teclado o el monitor. Su preocupación principal deberá ser que la unidad continúe trabajando de manera adecuada por periodos prolongados cuando esté bajo carga.

Usted también debe asegurarse de que la RAM funcione correctamente y que durante la prueba no resulten dañados ciertos sectores del disco. También es una buena idea que encienda y apague la unidad varias veces, puesto que el efecto del encendido en la unidad a menudo puede provocar una falla de algún componente.

Reconocimiento del servidor antes de implantar una mejora en el sitio

La familia de productos Windows 2000 aprovecha el hardware PnP (conéctese y utilícese), lo cual le permite detectar y, automáticamente, configurar cualquier dispositivo PnP para trabajar con Windows 2000 Server durante la instalación. Sin embargo, PnP no es perfecto. Por alguna razón, usted podría tener componentes instalados que no sean dispositivos PnP, pero Windows 2000 será capaz de configurar esos dispositivos. A veces, éstos pueden entrar en conflicto con otros dispositivos o, por alguna razón, los controladores de un dispositivo específico podrían no permitir la configuración apropiada. Debido a estas imperfecciones, es importante analizar los componentes instalados en el servidor antes de instalar Windows 2000 Server como una actualización. En realidad, no es importante llevar a cabo un análisis cuando se configure un nuevo servidor.

En el reconocimiento, tome nota de todos los dispositivos instalados, junto con los recursos que cada uno utiliza en el servidor. Los recursos incluyen el canal IRQ, el canal DMA y las direcciones I/O de memoria que utiliza cada dispositivo. Después, si un dispositivo no funciona correctamente después de que usted haya instalado Windows 2000 Server, podrá configurar el dispositivo en forma manual con parámetros conocidos que sí lo hagan.



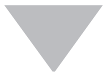
NOTA Algunos servidores vienen con utilerías, como SmartStart de Compaq, las cuales manejan el servidor en un nivel de hardware y mantienen la información en un espacio aparte del NOS. Las utilerías del servidor, como las de Compaq, le facilitan todo cuando trate de reparar un problema de hardware.

Toma de decisiones en la etapa de preinstalación

Después de configurar, verificar, preparar y probar su hardware, usted podrá comenzar la instalación de Windows 2000 Server. Durante este proceso, invierta un poco de su tiempo en tomar algunas decisiones importantes en la preinstalación que deberán estar preparadas para especificar durante la instalación. Las secciones siguientes analizan estas opciones.

¿Actualizar o instalar?

Usted puede actualizar un servidor que corra con Windows NT Server 3.51 ó 4.0 a Windows 2000 Server y conservar todos sus parámetros existentes, cuentas de usuario, permisos de archivos y cosas por el estilo. Asimismo, puede llevar a cabo una instalación completa que implique remover por completo cualquier NOS existente en el servidor. Usted deberá llevar a cabo una instalación completa en un nuevo servidor o en uno que corra cualquier NOS, que no sea Windows NT Server. Sin embargo, si utiliza una versión actualizable de Windows NT Server, existen ventajas y desventajas de ambas opciones.

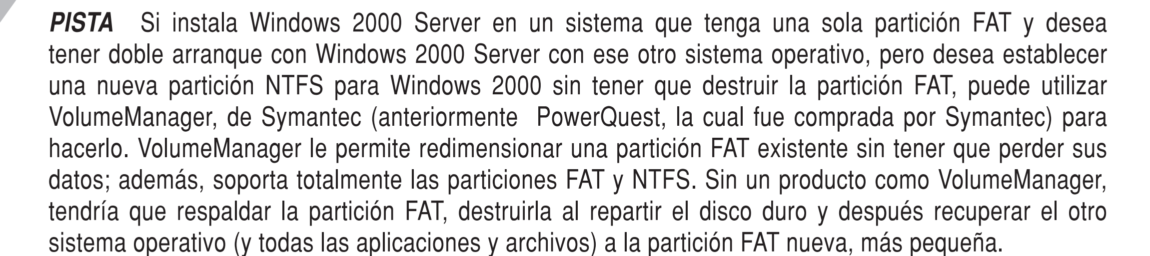


NOTA Si usted utiliza Windows NT Server 4 Enterprise Edition, solo puede actualizarla a Windows 2000 Advanced Server.

El principal beneficio de la actualización es que se conservarán todos sus parámetros existentes bajo Windows NT Server y automáticamente se transferirán a su instalación de Windows 2000 Server. Entre estos parámetros se encuentran detalles de conectividad de redes, como la información sobre la configuración de TCP/IP, así como los parámetros de seguridad que habrá tenido que configurar tediosamente a través del tiempo. En realidad, si el servidor pudiera actualizarse, sería buena idea que planeara hacerlo, a menos que necesitara modificar algo de primordial importancia en el servidor, como cambiar de FAT a NTFS.

¿FAT o NTFS?

Windows 2000 Server soporta discos duros formateados ya sea utilizando la tabla de localización de archivos (FAT16 y FAT32) o el sistema de archivos NT (NTFS). El uso de NTFS en Windows 2000 genera algunas ventajas importantes y, en algunos casos, son necesarias. Usted quizá desee instalar Windows 2000 Server en un disco que utilice el sistema de archivos FAT solo cuando el sistema deba utilizarse en una configuración de arranque dual, donde retiene la capacidad de arrancar otro sistema operativo, como el Windows 98. Sin embargo, aun en casos donde no necesite conservar la facilidad de doble arranque, usted estará mejor si conserva una partición FAT principal para el otro sistema operativo y configura una partición extendida con NTFS para almacenar el Windows 2000 Server. En dichos casos, Windows 2000 automáticamente instala el soporte al doble arranque que le permita seleccionar qué sistema operativo debe utilizar cuando el sistema arranque.



PISTA Si instala Windows 2000 Server en un sistema que tenga una sola partición FAT y desea tener doble arranque con Windows 2000 Server con ese otro sistema operativo, pero desea establecer una nueva partición NTFS para Windows 2000 sin tener que destruir la partición FAT, puede utilizar VolumeManager, de Symantec (anteriormente PowerQuest, la cual fue comprada por Symantec) para hacerlo. VolumeManager le permite redimensionar una partición FAT existente sin tener que perder sus datos; además, soporta totalmente las particiones FAT y NTFS. Sin un producto como VolumeManager, tendría que respaldar la partición FAT, destruirla al repartir el disco duro y después recuperar el otro sistema operativo (y todas las aplicaciones y archivos) a la partición FAT nueva, más pequeña.

Se requiere el NTFS para cualquier Windows 2000 Servers que funcione como controladores de dominio y también es el único sistema de archivos que le permite aprovechar totalmente las facilidades de seguridad del Windows 2000. Además, el NTFS se encuentra optimizado para el buen funcionamiento del servidor y se desempeña mejor que el FAT bajo casi cualquier circunstancia.

Controlador de dominio, servidor miembro o servidor independiente

Antes de contestar esta pregunta, necesita comprender dos conceptos importantes de las redes Windows 2000: dominios y grupos de trabajo. Un *dominio* es un complejo agrupamiento administrativo de computadoras en una red Windows 2000 que permite administrar los recursos de la red desde un solo punto e implantar una seguridad muy sólida. Los dominios le permiten administrar múltiples servidores Windows 2000 o Windows NT de una manera más fácil. Un *grupo de trabajo* es una simple colección de computadoras integradas en una red y es apropiada solo en redes de igual a igual.

Usted puede configurar Windows 2000 Servers en uno de los tres siguientes modos que soportan tanto a dominios como a grupos de trabajo:

- Los controladores de dominio almacenan la información del directorio activo del dominio y autentifican a los usuarios y el acceso a los recursos. La mayoría de las redes Windows 2000 tienen al menos un dominio y, por tanto, necesitan al menos de un controlador de dominio.
- Los servidores miembros son parte de un dominio, pero no conservan una copia de la información que contiene el directorio activo (Active Directory).
- Los servidores independientes no participan en un dominio, sino que lo hacen en un grupo de trabajo.

Antes de que apareciera Windows 2000, los servidores de Windows NT que eran controladores de dominio tenían que ser designados como controladores de dominio principal (PDC) o controladores de dominio de respaldo (BDC). Windows 2000 con el directorio activo simplifica las cosas de forma que todos los controladores de dominio Windows 2000 son simplemente eso. Cada uno de ellos mantiene una copia de la información del directorio activo y puede llevar a cabo todas las funciones de los demás controladores de dominio. Anteriormente, el PDC llevaba a cabo todas las tareas administrativas, mientras que los BDC simplemente conservaban copias de solo lectura de la información del dominio, a fin de continuar autentificando la seguridad de la red en caso de que el PDC fallara. Por otro lado, Windows 2000 Server utiliza el concepto de *controladores de dominio multimáster*, que operan de la misma forma que los demás controladores.



PISTA Excepto en la redes más pequeñas, es una buena idea contar con dos controladores de dominio. De esta manera, toda la información de su dominio se conserva y está disponible en la red en caso de que falle uno de los controladores. La información del dominio se sincroniza automáticamente entre los controladores de dominio disponibles.

¿Por sitio o por servidor?

Otra decisión importante que se debe tomar cuando se instala el Windows 2000 Server es cómo administrará el servidor sus licencias de acceso al cliente (CAL). Windows 2000 Server soporta dos formas diferentes de administrar CAL: por servidor o por sitio. Las *licencias por servidor* asignan las CAL al servidor, el cual permitirá solo tantas conexiones desde las computadoras como CAL haya instaladas en ese servidor. Las *licencias por sitio* requieren la compra de una CAL por cada una de las computadoras cliente, la cual les da el derecho de acceder a tantos servidores Windows 2000 como deseen; los servidores no supervisarán el número de conexiones. En general, Microsoft recomienda que utilice licencias por servidor cuando tenga un solo servidor y licencias por sitio cuando corra en múltiples servidores. Si usted no está seguro qué modo utilizar, Microsoft recomienda que seleccione por servidor ya que Microsoft le permite cambiar al modo por sitio una sola vez sin costo (mientras que el cambio de sitio por servidor tiene un precio). Revise cuidadosamente las opciones de licencia con su distribuidor Windows 2000 para determinar la forma más económica de adquirir licencias para los servidores de su red.

¡Espere! ¡Respalde antes de actualizar!

Si usted está instalando Windows 2000 Server como una actualización de otro NOS, como el Windows NT Server, es muy importante que respalde el servidor antes de instalar Windows 2000 Server. (Es una buena idea hacer dos respaldos idénticos, por si acaso). Usted debe utilizar cualquier software de respaldo que normalmente use para su NOS existente, asegurándose de que el software pueda restablecer adecuadamente el NOS anterior en caso de que necesite "regresar" el proceso de actualización e ir al punto donde comenzó el proceso. Incluso cuando lleve a cabo una actualización a Windows NT y no esté reformateando alguno de los discos, es bueno hacer un respaldo de la preinstalación en caso de que se presenten problemas.

INSTALACIÓN DEL WINDOWS 2000 SERVER

Existen muchas formas de comenzar la instalación de Windows 2000 Server. Usted puede:

- Configurar la computadora del servidor para iniciar desde el CD-ROM Windows 2000 Server.
- Comenzar la instalación al mismo tiempo que corre el Windows NT Server.
- Comenzar la instalación al mismo tiempo que se encuentra corriendo el Windows 95 ó 98.
- Preparar disquetes de arranque y utilizarlos para comenzar el proceso de instalación.
- Instalar desde un punto de instalación de la red que haya sido configurado previamente.

En realidad, cuando configure un servidor nuevo, usted tiene solo dos opciones para comenzar la instalación: arranque desde el CD-ROM Windows 2000 Server o prepare disquetes de arranque. La mayoría de los servidores pueden arrancar desde sus controladores de CD-ROM, la cual es la mejor forma de llevar a cabo la instalación. Si, en lugar de eso, necesita preparar disco de arranque, puede hacerlo corriendo el programa MAKEBOOT.EXE que se encuentra en el CD-ROM Windows 2000 Server. La instalación de ejemplo de este capítulo supone que usted arrancará el proceso de instalación desde el CD-ROM Windows 2000 Server.

Ejecución del programa de instalación de Windows 2000 Server

Las secciones siguientes describen el proceso de correr el programa de instalación de Windows 2000 Server y su instalación en el servidor. Si usted quiere aprender acerca de Windows 2000 Server y tiene una computadora apropiada que pueda utilizar, deberá tomarse un tiempo para instalar Windows 2000 Server, a fin de que conozca cómo trabaja el proceso. O, si así lo desea, puede leer las descripciones siguientes a fin de que se familiarice con el proceso de instalación. (En realidad, yo recomiendo hacer una instalación como la que se describe aquí y, después, "jugar con" el servidor resultante como una forma de aprender más rápida y completamente acerca de Windows 2000 Server).

Cuando usted arranque desde el CD-ROM del Windows 2000 Server, en primer lugar el programa le presentará una pantalla basada en texto que lo llevará por medio de las primeras opciones de instalación que tendrá qué hacer. Presione ENTRAR a fin de confirmar que desea instalar el Windows 2000 Server, o presione la tecla F3 para salir del programa de instalación.

Luego, el programa lo invita a seleccionar si desea instalar el Windows 2000 Server o reparar una instalación existente. Usted tiene que presionar ENTRAR para seleccionar la instalación del Windows 2000 Server.

A continuación, el programa le pregunta si está de acuerdo con el contrato de licencia de Windows 2000 Server. Presione F8 para contestar afirmativamente y proceda.

La pantalla siguiente comienza con lo más interesante del proceso de instalación. Usted verá una pantalla que enumera todas las particiones de disco disponibles a partir de las que puede instalar Windows 2000 Server. En este punto puede llevar a cabo las acciones siguientes:

- Utilice las teclas con flechas y presione ENTRAR para seleccionar una partición de disco existente.
- Presione la letra C del teclado para crear una nueva partición en el disco a partir de un disco no particionado. (Una nueva instalación de un servidor, en general, requiere que usted cree una partición).
- Presione la letra D en el teclado para eliminar una partición existente (usted deberá hacer esto solamente cuando quite todos los vestigios de un sistema operativo previo, después de lo cual podrá crear la instalación de la partición que usted necesite).

Cuando usted presione la letra C para crear una partición, el programa le pregunta sobre el tamaño de la partición que desea crear. Por omisión, el programa ofrece la partición de tamaño máximo. Para aceptar esta opción, simplemente presione ENTRAR, en cuyo punto el programa crea una nueva partición. Después, regresa a la pantalla que presenta todas las particiones y el programa despliega la nueva partición que usted creó como "Nueva (sin formatear)". Seleccione esta partición y presione ENTRAR para continuar.

Después de que seleccione la nueva partición, el programa lo invita a seleccionar un formato de disco, ya sea FAT o NTFS. En la mayoría de los servidores, usted utiliza solamente particiones NTFS, así que seleccione NTFS y presiones ENTRAR para continuar. En este punto, el programa de instalación formatea la partición por usted.

NOTA Un breve estudio acerca de la selección entre FAT y NTFS aparece en secciones anteriores en este capítulo, en la sección "¿FAT o NTFS?".

Después de que ha terminado el formateo, se copian automáticamente a la nueva partición los archivos necesarios para continuar la instalación de Windows 2000 Server. Después de que se copiaron los archivos, el programa reinicia el sistema de manera automática, así como la parte gráfica de la instalación.

El programa de instalación de los gráficos lo lleva por medio de varias opciones de instalación que usted debe elegir durante el proceso. Aunque pueda modificar la mayoría de estas opciones después, es mejor que tome las decisiones correctas desde el principio durante la instalación inicial de Windows 2000 Server. Lo que resta de esta sección continúa con el proceso de instalación en la computadora. Este proceso toma cinco o diez minutos.

Una vez que los dispositivos básicos están instalados y configurados, se le invita a seleccionar los parámetros locales y del teclado que usted desee. Estas opciones son por omisión: Inglés (de Estados Unidos) y la disposición de Teclado de Estados Unidos (si utiliza una copia de Windows 2000 Server adquirida en ese país), por lo que podrá, en general, seleccionar la opción Next para continuar.

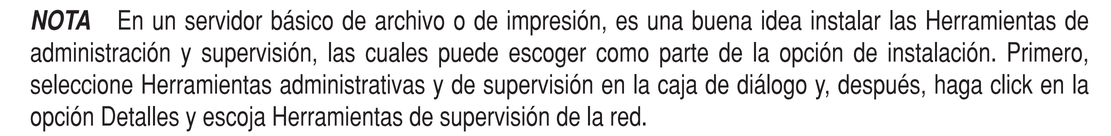
A continuación, el programa lo invita a ingresar su nombre y el de su empresa. La mayoría de las compañías prefiere que usted no personalice el sistema operativo con el nombre de una instancia en particular. En lugar de eso, utilice un nombre como "Departamento IT" y, después, ingrese el nombre de su compañía en el campo que se proporciona. Teclee Next para continuar.

La caja de diálogo que sigue es importante. En ella usted ingresa el nombre de la computadora en la que instala el Windows 2000 Server; además, también debe ingresar la contraseña inicial del administrador. El nombre de la computadora que seleccionó será el nombre del servidor, el mismo que verán los usuarios cuando naveguen por los servidores de la red. Si es posible, puede seleccionar un nombre que no necesite cambiar después. Para la contraseña del administrador, seleccione una fuerte y buena que no pueda adivinarse fácilmente. La contraseña del administrador es la clave para hacer todo lo que necesite con el servidor, por lo que debe seleccionar una contraseña que sea segura. Como regla, seleccione una contraseña de administrador con ocho o más caracteres, incluyendo letras y números. ¡Asegúrese de que sean una contraseña fácil de recordar! Después de haber terminado de llenar todos los campos, teclee Next para continuar.

Enseguida, el programa desplegará una caja de diálogo que presenta todos los diferentes componentes que podrá instalar opcionalmente con Windows 2000 Server. Si sigue este procedimiento y lleva a cabo una instalación de muestra de Windows 2000 Server para aprender acerca del proceso de instalación, solo deberá seleccionar las opciones básicas relacionadas con la instalación del servidor de impresión y de archivos. Sin embargo, a continuación se muestra una lista con todas las opciones (los componentes que puede agregar después de que la instalación principal se haya terminado):

- **Servicios de certificación (1.5 MB)** Los servicios de certificación se utilizan para habilitar aplicaciones de llave pública. Usted no necesita instalar esta opción a menos que tenga una aplicación que requiera estos servicios.
- **Servicios de agrupamiento (2.2 MB)** Los servicios de agrupamiento de Windows 2000 le permiten a dos o más servidores compartir una carga de trabajo común y ofrecer soporte contra fallas en caso de que uno de los servidores experimente una en el hardware. Usted no necesita instalar esta opción a menos que desee construir un agrupamiento de servidores con alto grado de disponibilidad.
- **Servidor de información de Internet (ISS) (28.7 MB)** IIS permite que una Windows 2000 Server trabaje como un servidor de web y FTP. Si selecciona esta opción se instala IIS junto con una serie de facilidades relacionadas con el mismo. Usted no necesita instalar el IIS para un servidor de archivo e impresión.
- **Herramientas administrativas y de supervisión (15.7 MB)** Si selecciona esta opción se instalan las herramientas administrativas complementarias, que incluyen las siguientes:
  - Los componentes del administrador de la conexión para administrar las conexiones RAS y conmutadas.
  - La herramienta de migración al servicio de directorio para migrar de Servicios de directorio de NetWare (NDS) al directorio activo de Windows 2000.

- Herramientas de supervisión de la red, que usted puede utilizar para llevar a cabo el análisis y la decodificación de paquetes de red rudimentarios.
- Protocolo simple de administrador de la red, el cual permite que Windows 2000 Server reporte información administrativa a una computadora SNMP de administración en la red.

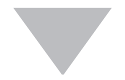


NOTA En un servidor básico de archivo o de impresión, es una buena idea instalar las Herramientas de administración y supervisión, las cuales puede escoger como parte de la opción de instalación. Primero, seleccione Herramientas administrativas y de supervisión en la caja de diálogo y, después, haga click en la opción Detalles y escoja Herramientas de supervisión de la red.

- **Servicios de cola de mensajes (2.4 MB)** Estos servicios ponen en la cola los mensajes de red que se utilizan en ciertas aplicaciones cliente/servidor. A menos que dicha aplicación le solicite hacer eso, no es necesario instalar esta herramienta.
- **Depurador de scripts de Microsoft (1.6 MB)** Esta opción agrega las herramientas que le permitirán depurar los scripts escritos en VBScript y en JScript. Debido a que ocasionalmente usted puede necesitar acceder a Internet a través de un navegador de la web en el servidor (para bajar actualizaciones de controladores, por ejemplo) y debido a que puede desarrollar scripts basados en VBScript o JScript, es mejor que opte por instalar esta herramienta.
- **Servicios de conectividad de redes (3.6 MB)** Esta opción es apropiada para una gran variedad de servicios de red que usted podrá instalar en su servidor. En particular, deberá considerar la selección de algunas de estas opciones en el caso de un servidor de impresión o de archivos. Primero, considere la instalación del protocolo de configuración de host dinámico (DHCP), el cual permite que el servidor administre una gran cantidad de direcciones IP y que asigne direcciones automáticamente a las computadoras cliente. Segundo, considere la instalación del servicio de nombres en Internet de Windows (WINS), el cual proporciona la resolución de nombres y el soporte de navegación a las computadoras cliente que corren sistemas operativos anteriores al Windows 2000 (como Windows NT y Windows 9x) y que utilizan solo el protocolo TCP/IP. Sin embargo, ninguna de estas opciones se requiere en un servidor de archivos o de impresión básico.
- **Otros servicios de archivo e impresión de red** Esta opción le permite instalar la ayuda adicional que se requiere para compartir los archivos y las impresoras del servidor con computadoras Macintosh y las que están basadas en UNIX. Usted no necesita seleccionar esta opción si todas sus computadoras cliente corren alguna versión de Windows.
- **Servicios de instalación remota (RIS) (1.4 MB)** Con los RIS, usted puede instalar remotamente Windows 2000 Professional en las computadoras de la red que soporten una facilidad llamada *arranque remoto*. Usted necesita una partición dedicada en el servidor para almacenar las imágenes de disco del Windows 2000 Professional, mas no necesita esta herramienta para un servidor básico de impresión o de archivos.
- **Almacenamiento remoto (3.5 MB)** Esta facilidad le permite configurar un disco de Windows 2000 Server para transferir automáticamente archivos que se acceden muy rara vez a un controlador de cinta o CD escribible. Si se necesitan, el sistema operativo

puede llamar automáticamente a estos archivos. La mayoría de los servidores no necesitan esta herramienta.

- **Servicios de terminal (14.3 MB) y licencia de los servicios de terminal (0.4 MB)** Estas dos opciones le permiten al Windows 2000 Server almacenar múltiples sesiones de Windows de computadoras remotas, en las que las aplicaciones se ejecuten en el servidor y la computadora del cliente maneje solo la entrada de la pantalla y el teclado/mouse para la aplicación. Los servicios terminales de Windows trabajan de forma similar a las computadoras grandes, donde todo el trabajo se lleva a cabo en la computadora grande y el cliente actúa solo como una terminal de una computadora grande. Usted no necesita estas opciones para los servidores de archivos o de impresión.



PISTA La comprensión y administración de los servicios terminales pueden ser tareas complicadas y requieren ciertas técnicas que no son evidentes a primera vista. Tomar un curso o comprar un libro acerca de los servicios terminales es probablemente una buena sugerencia, especialmente si usted los utiliza como un control remoto exclusivo o una solución de acceso remoto.

Después de hacer una selección a partir de las opciones anteriores, teclee Next para continuar. El programa le pedirá información acerca de un módem conectado al servidor, si es que existe. Usted puede proporcionar su código de área y cualquier número que necesite marcar para acceder a una línea hacia el exterior e indicar si la línea telefónica soporta marcación por tonos o por pulsos. Llene los campos que se le solicita y teclee Next para continuar.

A continuación, el programa le solicita ingresar la fecha y hora correctas, así como la zona de tiempo en la que reside el servidor. Actualice estos campos si fuere necesario y teclee Next.

Luego, el programa lo invita a seleccionar sus parámetros de red. Usted puede seleccionar entre los parámetros típicos y los del cliente. Para una red pequeña, podrá seleccionar la primera opción sin ningún problema. La segunda opción le permite definir detalles como qué componentes de conectividad de redes se instalarán y cómo está configurado cada uno. Para este ejemplo de una instalación básica de Windows 2000 Server, se selecciona la opción Parámetros típicos.

Instalación de Windows 2000 Server

En este ejemplo, usted va a instalar el Windows 2000 Standard Server en una computadora que corre Windows Me. Ésta es una buena forma de aprender acerca de Windows 2000 Server sin tener que contar con una computadora para que lo corra. Cuando haya terminado, usted será capaz de arrancar ya sea con Windows 98 (u otros sistema operativos Win9x, como Windows Me) o con Windows 2000 Standard Server.

1. En la computadora que tiene ya instalada una versión anterior de Windows, asegúrese de que tenga la capacidad apropiada para instalar y correr Windows 2000 Server. Este tema se analizó anteriormente: básicamente la computadora debe tener un procesador Pentium a 133 MHz o uno más rápido, 256 MB de RAM, y aproximadamente 1 GB de espacio libre en disco.

2. Inserte el CD-ROM Windows 2000 Server CD-ROM y arranque la computadora desde el controlador de CD-ROM. (En algunas computadoras, usted tendrá que cambiar los parámetros del BIOS para permitir al arranque desde el CD-ROM).

3. Lea la parte textual del proceso de instalación. Cuando se le solicite una partición de disco en la que se instalará Windows 2000 Server, usted puede seleccionar cualquier partición disponible en el disco que tenga espacio suficiente, incluyendo la que ya contiene a Windows; Windows 2000 Server instalará y correrá en una partición FAT o FAT32 formateada. Sin embargo, si tiene una partición disponible que no le importe borrar, puede dar formato a esa partición con NTFS e instalar Windows 2000 Server en ella. Siempre y cuando la partición principal no sufra modificación alguna, el arranque doble funcionará en esta configuración.

4. Reinicie la computadora en la parte final de la instalación que se basa en texto a fin de comenzar con la porción gráfica de la instalación.

5. Continúe y responda las preguntas básicas que se solicitan durante el comienzo de la instalación gráfica, como la selección de un sitio y un teclado e ingrese su nombre.

6. Cuando se lo solicite el sistema, seleccione Licencia por sitio para un servidor independiente para aprendizaje.

7. Cuando se le pida, ingrese un nombre para este servidor (el nombre por medio del cual el servidor será visto por la red) y asigne una contraseña del administrador (asegúrese de que sea una que no vaya a olvidar).

8. Cuando se le pida, tome las decisiones apropiadas acerca de qué servicios de Windows 2000 Server va a instalar. Para un buen servidor genérico en el cual comenzar por aprender acerca de Windows 2000 Server, seleccione el Servidor de información de Internet, Herramientas administrativas y de supervisión y los Servicios de conectividad de redes.

9. Termine lo que resta de la instalación, seleccionando Típica cuando se le pida la parte de conectividad de redes de la instalación del servidor y ya sea Servidor del controlador de dominio o Servidor independiente, cuando se le pida ingresar el tipo de servidor. NO seleccione Controlador de dominio si está llevando a cabo esta instalación en la red de una compañía en operación, sin consultar primero al administrador de la red (y probablemente ni aun así evitará causar problemas en la red). Sin embargo, si usted está utilizando una pequeña red casera, puede experimentar y trabajar con un Controlador de dominio seleccionando esa opción.

Después de que haya terminado la parte gráfica de la instalación, se le solicitará reiniciar la computadora. Cuando lo haga, usted verá un menú que le permitirá seleccionar arrancar ya sea con Windows 2000 Server (está será la opción por omisión), o con la versión existente de Windows.

Enseguida, el programa le pide seleccionar entre configurar Windows 2000 Server como miembro de un grupo de trabajo o como un dominio. En la sección: "¿Controlador de dominio, servidor de miembros o servidor independiente?", se presenta un análisis acerca de las diferencias entre las dos opciones. Sin embargo, usted no podrá asignar un nuevo servidor a un dominio a menos que éste ya exista y que un controlador de dominio esté disponible para autentificar (permitir) que el nuevo servidor ingrese al dominio. En el caso de un servidor nuevo, incluso uno que vaya a ser el controlador de dominio, seleccione Grupo de trabajo y teclee Next para continuar.

En este punto, el programa terminará esta parte de la instalación de Windows 2000 Server, utilizando la información que usted proporcionó.

Fin de la instalación de WINDOWS 2000 Server

Después de que se ha terminado el programa de instalación principal, el sistema reinicia en donde le pide la contraseña de acceso de Windows 2000 Server. Para acceder al servidor, presione CTRL-ALT-DEL. De esta forma ingresa como Administrador, utilizando la contraseña que usted definió como parte del proceso de instalación. Entonces, el escritorio de Windows 2000 Server aparecerá, junto con el programa Windows 2000 Configure Your Server (llamado programa de Configuración del servidor en lo que resta de esta sección), y lo conducirá por los pasos requeridos que faltan para hacer funcionar el servidor. La figura 16-1 muestra el programa de Configuración del servidor corriendo en el escritorio de Windows 2000.



Figura 16-1. Programa Windows 2000 Server Configuration.

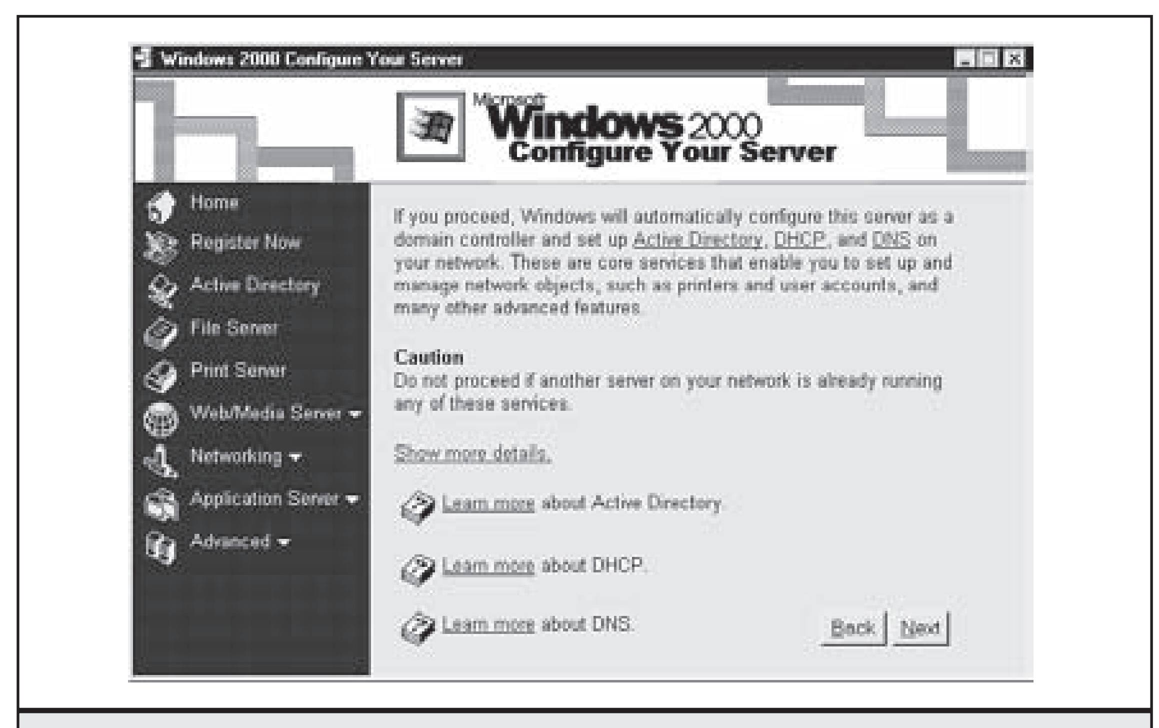


Figura 16-2. Confirmación de la instalación de los servicios de red principales.

Si usted está instalando un solo servidor en una red pequeña —suposición en que se basa el ejemplo de este capítulo— puede seleccionar la opción marcada: "Éste es el único servidor en mi red", como se muestra en la figura 16-1. Si la instalación es más complicada, seleccione "Ya existe uno o más servidores trabajando en mi red", lo cual requiere poseer un conocimiento más a fondo acerca de la instalación.

Después, verá una pantalla de confirmación (que se muestra en la figura 16-2) que confirma que desea instalar en el servidor los servicios de Directorio activo, de DHCP y de DNS, los cuales son estándar para un solo servidor de una red. Si usted lo desea, puede leer más acerca de estos servicios seleccionando los enlaces que se muestran en la caja de diálogo Server Configuration. Una vez que haya terminado, seleccione Next para continuar.

Enseguida, el programa le solicita el nombre del dominio que creará y cualquier dominio de Internet del que el servidor deba estar enterado. El nombre de dominio no puede tener espacios y deberá seleccionar un nombre simple, uno con el que pueda trabajar fácilmente. Muchas compañías seleccionan el nombre de su empresa o alguna abreviatura de la misma como nombre de dominio. Usted también debe ingresar ahí cualquier dominio de Internet que exista en su red. El nombre de dominio de Internet es propiedad de su compañía. Por ejemplo, si trabaja para una compañía llamada Acme Corporation, puede llamar a su dominio de Windows 2000 ACME, y su dominio de Internet probablemente será acme.com. (Si su compañía no tiene un nombre de dominio, ingrese **local** en el campo). En el caso de este ejemplo, el nombre de dominio de Windows 2000 será OHM y el nombre de dominio de Internet será local. Ingrese su información y

teclee Next para continuar. Después de una pausa, el programa le advertirá que las selecciones que ha hecho se instalarán y que el servidor se reiniciará. Teclee Next una segunda vez para que esto suceda. Observe que su programa le pedirá el CD-ROM del Windows 2000 Server durante este proceso.

Después de que el sistema instale los componentes necesarios y se reinicie, usted necesita dar algunos pasos finales en el programa Server Configuration, después de los cuales habrá terminado de instalar el servidor. Siga los pasos siguientes:

1. Presione el botón derecho del mouse sobre el objeto del escritorio My Network Places y seleccione Properties del menú que se muestre.
2. Presione con el botón derecho del mouse el objeto Local Area Connection y seleccione Properties del menú que se despliegue. Si lo hace, se abrirá la caja de diálogo Local Area Connection Properties, que se muestra en la figura 16-3.
3. Seleccione la opción Internet Protocol y teclee el botón Properties.
4. Teclee el botón Use the Following IP Address.
5. Teclee el número IP correcto de este servidor para que se utilice como su dirección IP. Si usted no cuenta con un rango de números y su red no se encuentra conectada directamente a Internet, utilice la dirección 10.10.1.1.

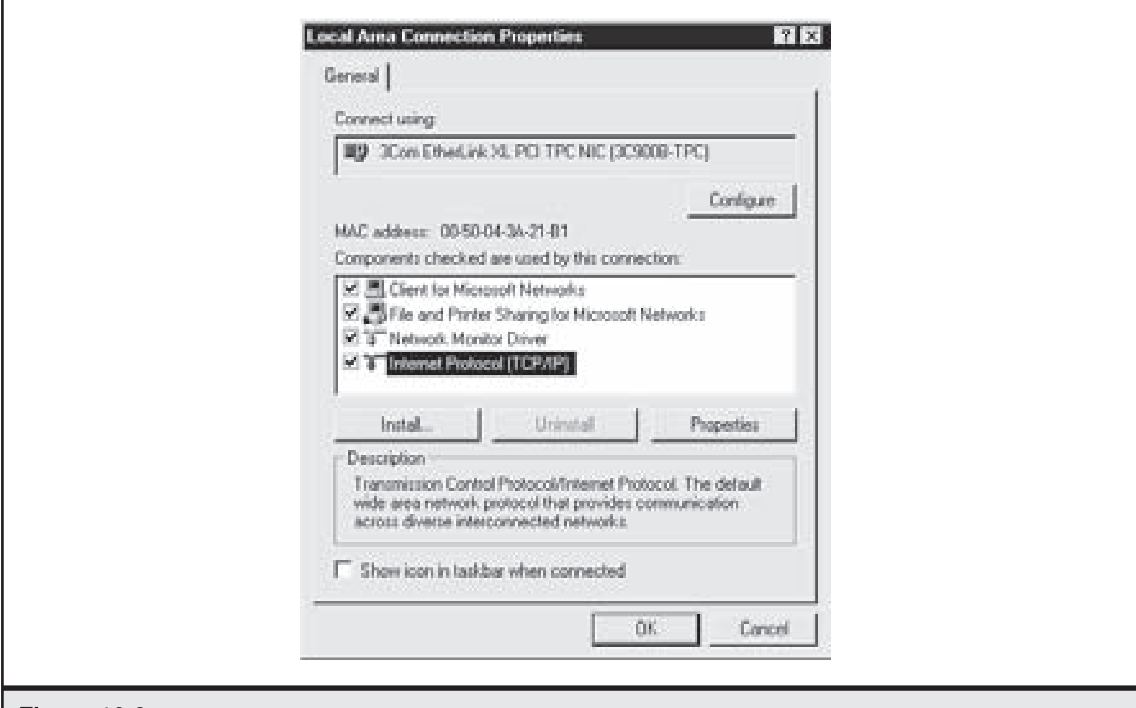


Figura 16-3. Caja de diálogo Local Area Connection Properties.

6. Teclee la máscara de subred correcta. Si anteriormente su red no ha utilizado máscaras de subred, seleccione 255.0.0.0.
7. En el campo Preferred DNS Server, ingrese la dirección IP que acaba de asignarle al servidor. En este ejemplo, se utiliza 10.10.1.1. En este punto, la caja de diálogo Internet Protocol (TCP/IP) Properties se deberá ver como se muestra en la figura 16-4. Teclee OK para cerrar las diferentes cajas de diálogo Properties que se encuentran abiertas.
8. Ahora necesita autorizar los servicios DHCP. Abra el menú Start y, después, seleccione Programs, Administrative Tools y DHCP. A continuación, se podrá ver el programa DHCP Manager como se muestra en la figura 16-5.
9. Expanda el árbol del lado izquierdo de la ventana. Después, con el botón derecho del mouse, haga click en el servidor que se muestra en ese lado de la ventana, seleccione All Tasks y después Authorize. Esta acción autoriza al servidor a responder las solicitudes del DHCP y le permite asignar direcciones IP a las computadoras cliente de la red.
10. Apague y vuelva a encender el servidor a fin de que surtan efecto estos cambios.

¡Felicidades! Finalizar este proyecto significa que usted ha terminado la configuración de un Windows 2000 Server que actúa como Controlador de dominio. Ahora cuenta con un servidor que es capaz de satisfacer las necesidades de muchos usuarios y de llevar a cabo un gran número de tareas de gran utilidad.

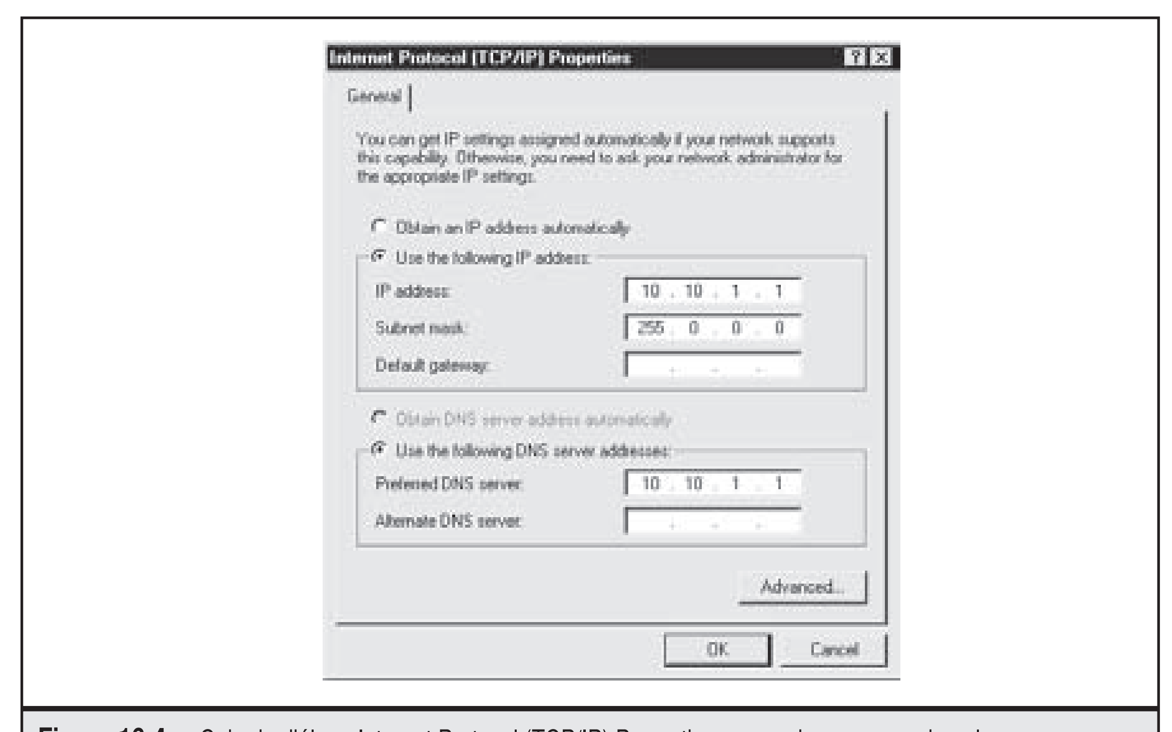


Figura 16-4. Caja de diálogo Internet Protocol (TCP/IP) Properties con opciones como ejemplo.

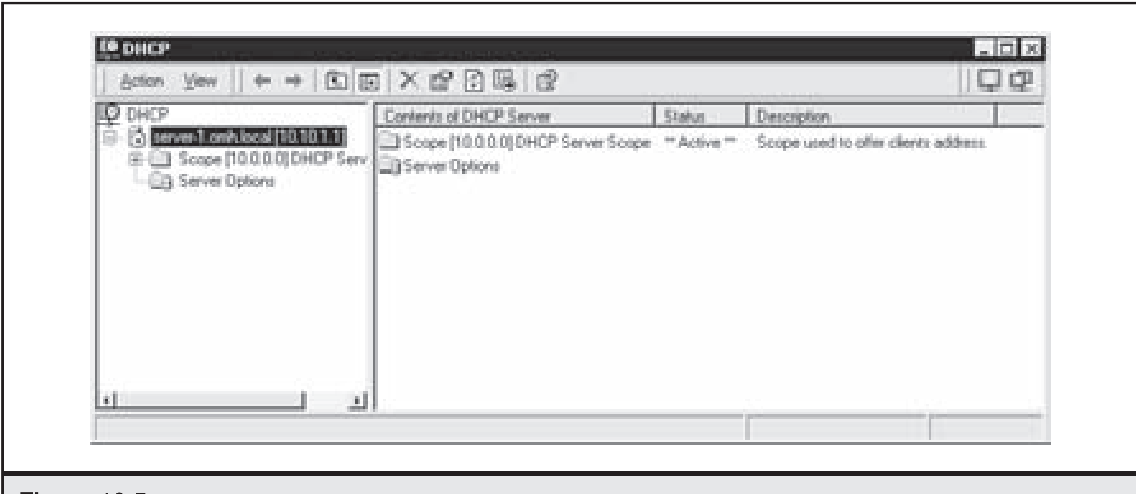


Figura 16-5. Programa DHCP Manager.

CONFIGURACIÓN DE UN SERVIDOR CLIENTE

Antes de que pueda terminar *realmente* la instalación de un nuevo servidor, necesita poner a prueba su capacidad para permitir que las computadoras cliente se conecten a él. Para llevar a cabo esta tarea, usted necesita cubrir los pasos siguientes:

1. Crear una cuenta de usuario de prueba.
2. Crear un recurso compartido en el servidor para que la computadora cliente puede acceder a él.
3. Configurar un cliente Windows 9x para conectarlo al servidor.
4. Firmar en el servidor, realmente, en la computadora cliente y verificar que todo trabaje correctamente.

Las secciones siguientes explican cómo llevar a cabo estas tareas.

Creación de una cuenta de usuario

La primera orden de negocios para confirmar la funcionalidad del servidor es crear una cuenta de usuario de prueba, con la que pueda registrarse en el servidor desde cualquier computadora de la red. Usted puede utilizar la cuenta del Administrador para hacerlo si desea saltarse este paso, pero utilizar una cuenta de usuario de muestra es mejor.

Comience abriendo el menú Start, después Programs y después Administrative Tools. Por último, seleccione la opción llamada Active Directory Users and Computers. Lo anterior abre la aplicación Windows Management Console con los parámetros del Active Directory Users and Computers, como se muestra en la figura 16-6.

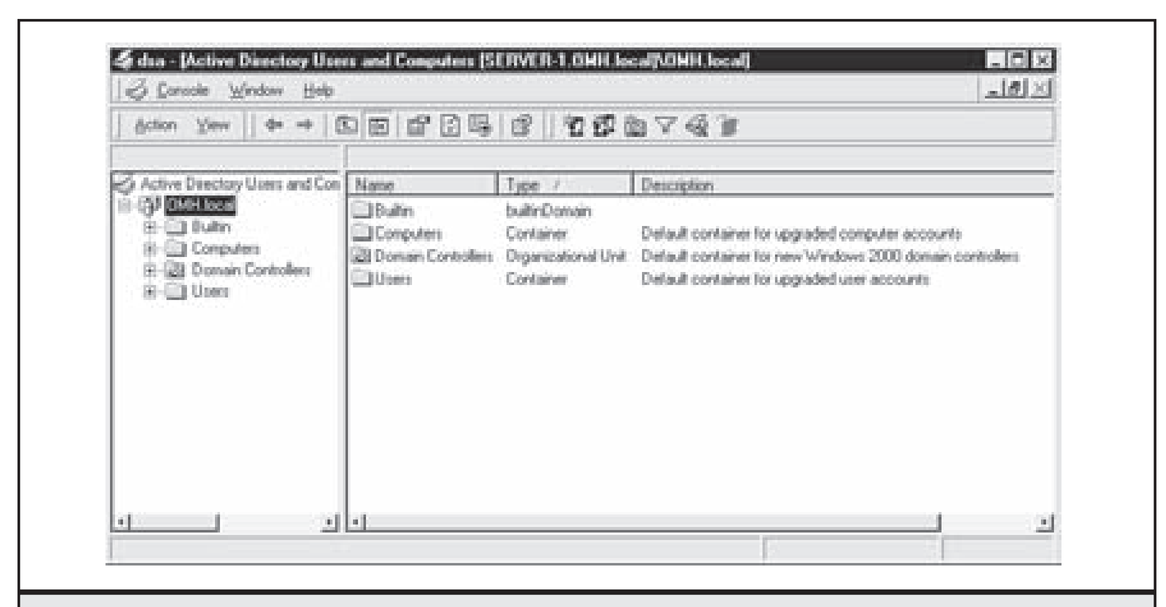


Figura 16-6. Usuarios y computadoras del directorio activo.

Como en la mayoría de los programas de Windows, el lado izquierdo de la ventana le permite navegar en el árbol (en este caso, el árbol de los objetos usuario y computadora) y el lado derecho muestra los detalles de la rama seleccionada. Para agregar un usuario, haga click con el botón derecho sobre el lado izquierdo de la ventana, seleccione New y, después, User del menú que se muestra. A continuación verá la caja de diálogo Create New Object (User) que se muestra en la figura 16-7.

Ingrese el nombre y el apellido del usuario que usted desee crear y, después, el nombre de registro en el campo User Logon Name. El programa genera los campos restantes de forma automática con base en la información que acaba de ingresar, aunque usted puede cambiar sus parámetros si así lo desea. En el ejemplo que se muestra en la figura 16-7, el usuario FredF se firmará en el Active Directory utilizando la cuenta de usuario **fredf@omh.local**. Después de ingresar la información, haga click en Next para continuar.

Ahora ingrese una contraseña de inicio para la cuenta que usted acaba de crear. En este ejemplo, simplemente utilice la contraseña **contraseña**. (Recuerde quitar esta cuenta de usuario de prueba después de que haya terminado de hacer las pruebas. Usted nunca querrá dejar una cuenta de usuario activa en el sistema con una contraseña que otros puedan adivinar fácilmente). Haga click en Next para continuar y, después, en Finish para terminar de crear la cuenta de usuario.



Figura 16-7. Caja de diálogo Create New Object (User).

Creación de un fólder compartido

El siguiente paso es crear un recurso —en este caso un fólder— al que el usuario de prueba pueda acceder desde una computadora de la red. El Windows 2000 Server comparte fólders mediante un mecanismo llamado *compartición*. Una *compartición* es un recurso navegable al que pueden acceder los usuarios remotos, siempre y cuando cuenten con los privilegios suficientes para hacerlo.

Para crear un fólder que pueda accederse a través de la red, genere un fólder normal en uno de los controladores de disco del servidor. Haga click con el botón derecho en el fólder y seleccione Sharing en el menú que se muestre, el cual desplegará la pestaña Sharing en la caja de diálogo Properties del fólder, como se muestra en la figura 16-8.

Para compartir el fólder, primero haga click en la opción Share this folder. Enseguida, revise el nombre compartido (el cual se asigna de manera automática con base en el nombre del fólder) y modifíquelo si así lo desea. Después, haga click en OK para terminar de compartir el fólder.



PISTA Por omisión, las comparticiones nuevas que se crean en el servidor le permiten a toda persona tener control total de su contenido. Para modificar este valor por omisión, es necesario que usted haga click en el botón Permissions y, después, modifique los permisos. Este procedimiento se estudia con más profundidad en el capítulo 17.

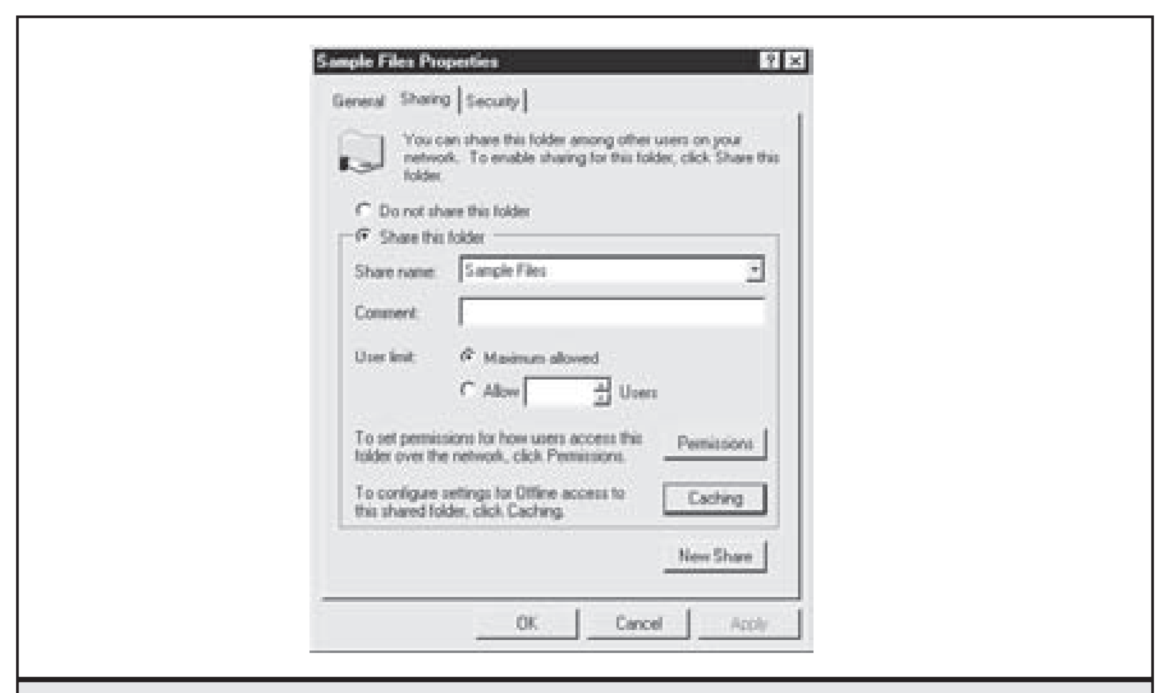


Figura 16-8. Pestaña Sharing de la caja de diálogo Properties de un fólder.

Configuración de un cliente Windows 9x para acceder al servidor

Para configurar un cliente Windows 95 o Windows 98 para acceder el nuevo servidor, siga los pasos siguientes:

1. En el Panel de control abra el objeto Network, con lo cual se activará la caja de diálogo Network.
2. Haga click en el botón Add, seleccione Client en la caja de diálogo Select Network Component Type y, después, haga click en Add para abrir la caja de diálogo Select Network Client.
3. En la caja de diálogo Select Network Client seleccione Microsoft de la lista de fabricantes y, después, seleccione Client for Microsoft Networks en el lado derecho de la ventana (vea la figura 16-9). Haga click en OK para continuar.
4. Después de un breve momento, la caja de diálogo Network reaparecerá al frente y se verán instalados el Client for Microsoft Networks y el TCP/IP protocol, como se muestra en la figura 16-10.
5. Seleccione Client for Microsoft Networks y haga click en el botón Properties.

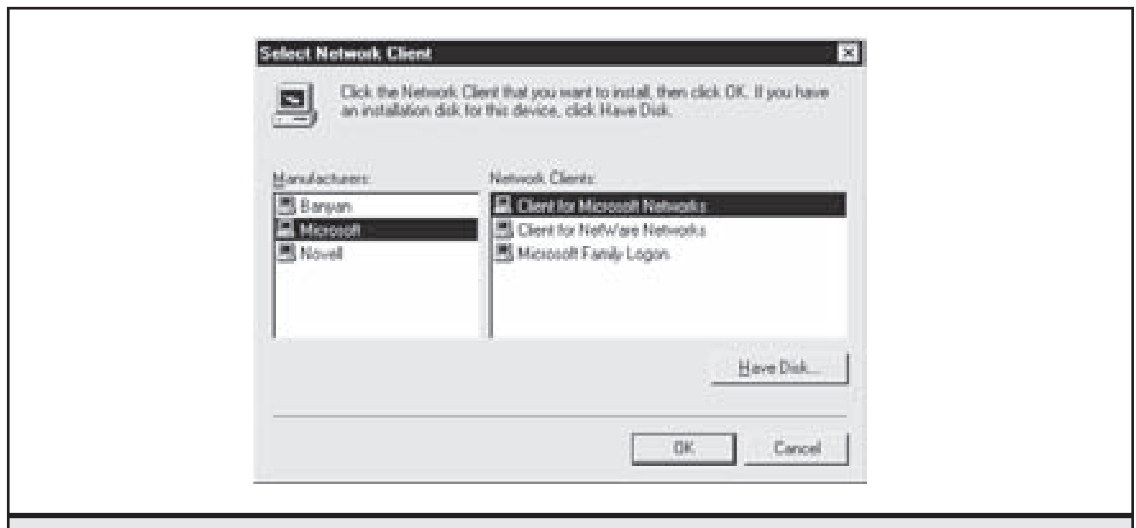


Figura 16-9. Selección de la instalación de Client for Microsoft Networks.

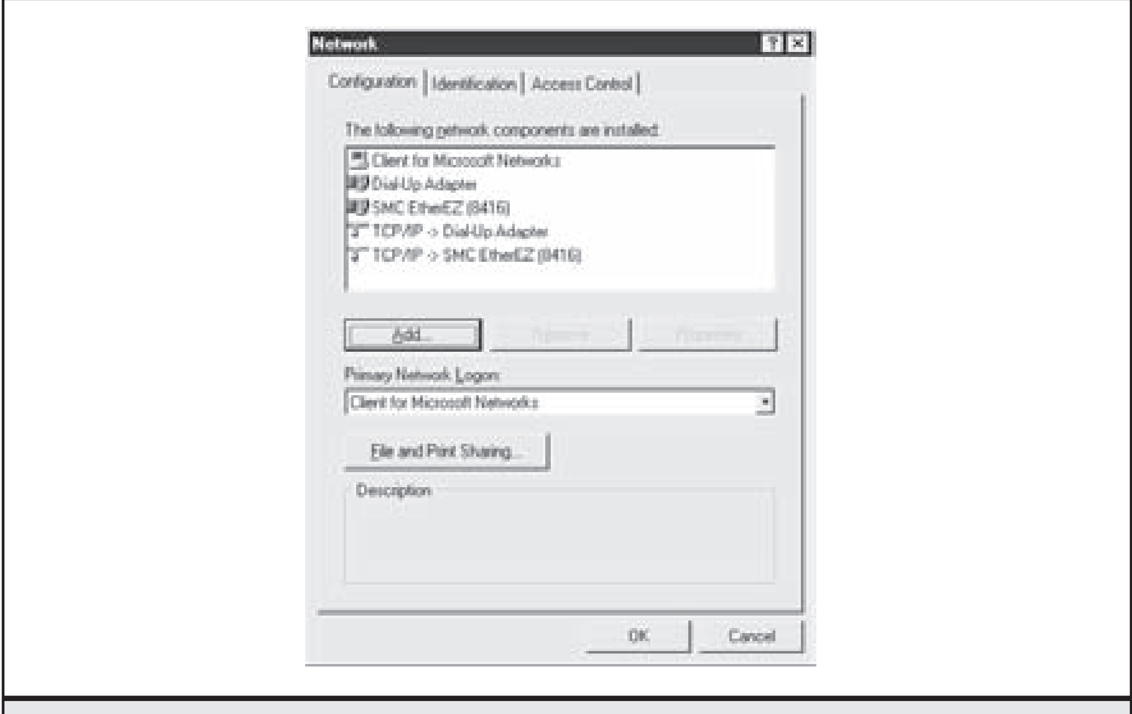


Figura 16-10. Caja de diálogo Network con componentes instalados.

6. En la caja de diálogo Client for Microsoft Networks Properties, seleccione la casilla de selección Log Onto Windows NT Domain y, después, teclee el nombre del dominio en el campo que se proporciona. En el ejemplo que se utilizó, el nombre del dominio es simplemente OHM.
7. Haga click en OK para cerrar la caja de diálogo Network.

Una vez que cierre la caja de diálogo Network, es probable que se le solicite su CD-ROM de Windows 9x a fin de que puedan instalarse los componentes necesarios. Después de que se haya terminado la instalación de los componentes de la red, el programa le solicitará reiniciar la computadora, lo cual usted deberá hacer antes de que se activen los parámetros de la red.

Prueba de la conexión del cliente

Usted podrá probar el servidor instalado ya sea mediante una computadora con Windows XP o Windows 2000 Professional que sea parte de la red, o una computadora Windows 9x que tenga agregados los servicios de conectividad de redes como se explicó en las instrucciones anteriores. Los pasos reales que se muestran aquí son los mismos para todos los sistemas operativos cliente de Windows más recientes.

Para probar el servidor, ingrese al dominio que está siendo administrado por Windows 2000 Server y navegue por los archivos que usted colocó en el fólder compartido.

Cuando reinicie la computadora después de que haya terminado los pasos de la sección anterior, el programa lo invita a ingresar al dominio antes de desplegar el escritorio de Windows 9x. Ingrese el nombre de la cuenta de usuario de prueba (**FredF**), el nombre del dominio (**OHM**), y la contraseña que usted asigna (***contraseña***) para ingresar en el dominio. Si usted ha ingresado la información correctamente, podrá ingresar al dominio. Si se presenta cualquier problema, como que no se pueda reconocer un nombre de usuario, una contraseña y un nombre de dominio, el programa le advertirá y le dará la oportunidad de corregirlo.

Una vez que inicie el cliente de Windows, usted debe poder abrir Network Neighborhood (o My Network Places, dependiendo de qué versión de Windows esté utilizando) y ver el servidor que instaló incluido en la lista de servidores. Cuando abra el servidor, podrá ver cualquier compartición en él a los cuales pueda acceder. Entre esos fólders, verá netlogin y sysvol, así como el que usted creó y compartió. Sin embargo, deberá ser capaz de abrir la compartición de ejemplo y ver los archivos que ha colocado en el fólder, así como manipularlos, eliminarlos, abrirlos, etc., como si estuviera trabajando con archivos en un disco duro local.



PISTA A veces, es posible que un servidor no aparezca automáticamente en Network Neighborhood, en particular si ha sido instalado recientemente. Si se topa con este problema, abra el menú Start, seleccione Find y, después, seleccione Computer. Teclee al nombre del servidor que esté instalando en la caja de diálogo Find y haga click en Find Now. Después de un momento, deberá aparecer el servidor en la caja de diálogo Find y podrá hacer doble click para abrirla.

RESUMEN DEL CAPÍTULO

En este capítulo, usted vio cómo se instala y configura Windows 2000 Server, utilizando opciones básicas de instalación que serán adecuadas para muchos servidores en pequeños negocios. Usted también aprendió cómo instalar y probar una computadora cliente para verificar que la red y el servidor trabajen perfectamente.

El propósito de este capítulo es familiarizarlo con los procedimientos básicos de instalación de Windows 2000 Server. Sin embargo, no abarca todas las opciones disponibles durante la instalación de Windows 2000 Server, pues no analiza temas de instalación más complejos que sean adecuados para redes más grandes. En lugar de eso, el objetivo de este capítulo es ayudar a los principiantes en la conectividad de redes a que comprendan las etapas básicas de la instalación de Windows 2000 Server y enseñarles lo suficiente que les posibilite poner en operación un servidor con un mínimo de problemas.

Si usted va a instalar Windows 2000 Server en un medio ambiente de producción —sin importar qué tan pequeño sea— es muy importante que aprenda mucho más acerca de Windows 2000 Server, así como de su instalación y configuración, de los que este libro abarca. Por fortuna, se encuentran disponibles muchas clases y libros muy buenos que le pueden enseñar todo lo que debe hacer para instalar y administrar una red basada en Windows 2000 Server.

La instalación del NOS es solamente una parte del proceso. Aún más importante es que usted conozca cómo administrar el servidor y llevar a cabo las diferentes tareas administrativas del NOS. Éstas incluyen la administración de las cuentas de usuario, los grupos, las impresoras y otras tareas de mantenimiento que se requieran. El capítulo 17 analiza los fundamentos de la administración de Windows 2000 Server. El capítulo 18 termina el estudio de Windows 2000 Server enseñándole acerca de las diferentes facilidades que incluye, como los Servicios de grupo, el Servidor de información de Internet, etcétera.

CAPÍTULO 17

Administración de Windows 2000 Server: los fundamentos

La instalación y configuración de Windows 2000 Server es solo la punta del iceberg. El proceso de administrar el servidor es más importante y consume una mayor cantidad de tiempo. Este proceso incluye tareas cotidianas y regulares, como la adición de nuevos usuarios, la eliminación de los antiguos, la asignación de permisos, la realización de respaldos, etc. Estos temas son la parte medular de este capítulo. Aprender cómo llevar a cabo todas estas actividades y hacerlas bien asegurará que la red y el servidor se mantengan productivos y seguros.

COMENTARIOS SOBRE LA SEGURIDAD DE LAS REDES

Antes de profundizar en las actividades administrativas que se estudian en este capítulo, usted deberá invertir más tiempo para pensar acerca de la seguridad de la red y de qué manera ésta se relaciona con su compañía. La seguridad es un tema importante y la administración de un servidor debe basarse en la conservación de la seguridad adecuada para su red.

La clave es recordar que cada red tiene un nivel de seguridad adecuado. Los requisitos de seguridad de un proveedor del Departamento de Defensa (DoD) que diseñe equipo militar serán diferentes de los requerimientos de seguridad de una compañía que opere restaurantes. Por tanto, el aspecto importante es, primero, determinar las necesidades de seguridad de su red. Muchos administradores principiantes pasan por alto este aspecto básico y configuran sus redes con las medidas de seguridad más exigentes que encuentran disponibles. El problema con esta forma de actuar es que estas medidas casi siempre reducen la productividad de quienes utilizan la red. Es necesario que haga un balance entre productividad y seguridad y la respuesta será diferente en cada compañía.

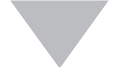
Por ejemplo, Windows 2000 Server le permite establecer diferentes políticas de seguridad para aplicar a los usuarios que incluyen forzar cambios en las contraseñas a intervalos que usted especifique, que las contraseñas tengan una cierta longitud mínima, que las nuevas siempre sean únicas y no reutilizar las contraseñas anteriores, etc. Usted podría establecer estas políticas a fin de que las contraseñas fueran de al menos 20 caracteres y que fueran modificadas semanalmente. Si los usuarios no recurrieran a escribir en papel sus contraseñas a fin de poderlas recordar de una semana a otra, estos parámetros serían más seguros que las contraseñas más cortas, cambiadas con menos frecuencia. Una contraseña de 20 caracteres es virtualmente imposible de violar utilizando métodos estándar y los cambios semanales de ellas reducen la probabilidad de que alguien la adivine y pueda utilizarla por un largo periodo. Sin embargo, el problema con políticas tan estrictas es que los usuarios olvidarán sus contraseñas con mucha frecuencia, serán sacados del sistema por periodos prolongados y requerirán mucha ayuda de parte del administrador de red (¡usted!) para solventar estos problemas cada vez que se presenten. Para un proveedor del DoD, todas estas complicaciones puede ser que valgan la pena. Sin embargo, en el caso de un operador de restaurantes, serían inadecuadas y terminarían por dañar a la compañía más que ayudarla. Por tanto, el punto que debe recordar es que la seguridad de la red siempre debe considerar el tipo de compañía y su red en particular, y que es importante definir los niveles de seguridad apropiados desde el principio y obtener el soporte necesario de la alta dirección para tomar las decisiones que piense que sean apropiadas.

Un aspecto relacionado con esta cuestión es que algunas veces una seguridad muy estricta da como resultado una reducción de la seguridad a largo plazo, al menos en ciertos aspectos. Así, en el ejemplo anterior en el que se manejan contraseñas de 20 caracteres que cambian muy a menudo, usted puede estar seguro de que un gran porcentaje de usuarios tendrán que escribir sus contraseñas a fin de recordarlas y poder acceder al sistema. Por supuesto, el problema aquí es que una contraseña escrita es mucho menos segura que una que se ha memorizado, ya que alguien puede encontrarla y, después de eso, violar la seguridad fácilmente.

El punto final —y la razón por la que usted debe poner atención a este tema antes de aprender acerca de administración— es que debe determinar la seguridad de red apropiada en una etapa inicial, a fin de que dé cabida a hacerlo, a medida que usted administra la red diariamente. La seguridad de la red no debe tomarle mucho tiempo, siempre y cuando establezca sus procedimientos administrativos de forma que presupongan los niveles de seguridad que usted requiere. Por ejemplo, si conoce cuáles serán sus políticas en cuanto a contraseñas en la red, solo le tomará unos segundos asegurarse de que cada nuevo usuario las conozca y las establezca en su cuenta. Si sabe que mantiene un reporte en papel de los cambios en los grupos de seguridad de la red, entonces tomará solamente un segundo seguir este procedimiento a medida que, ocasionalmente, cambien los miembros del grupo. El hecho de no determinar estas prácticas y políticas de seguridad en una primera fase traerá como resultado tener que involucrarse en proyectos más grandes como parte de una auditoria o una revisión de seguridad. ¡Seguridad es un área donde estará más a gusto si hace las cosas correctamente desde el principio!

TRABAJO CON CUENTAS DE USUARIO

Para que todos —incluyendo al administrador— puedan acceder a Windows 2000 Server, él o ella deberán contar con una cuenta establecida en el servidor o en el dominio. (Un dominio es una colección de información sobre seguridad compartida entre servidores Windows 2000). La cuenta define el *nombre del usuario* (el nombre con el que el sistema reconoce al usuario) y la contraseña de usuario, junto con gran cantidad de información específica de cada uno. La creación, el mantenimiento y la eliminación de cuentas de usuario son fáciles con Windows 2000 Server.



NOTA A cada cuenta que se crea para un dominio Windows 2000 Server se le asigna un número especial, llamado ID de Seguridad (SID). En realidad, el servidor reconoce al usuario por este nombre. Se dice que los SID son "únicos en el espacio y en el tiempo". Esto significa que ningún par de usuarios jamás tendrán el mismo SID, aun cuando tengan el mismo nombre de usuario o la misma contraseña. Esto se debe a que el SID está formado por un número único asignado al dominio y, por tanto, un número secuencial asignado a cada cuenta creada (con miles de millones de número únicos específicos de usuario disponibles). Si usted tiene un usuario llamado Frank, elimina esa cuenta y después crea otra cuenta llamada Frank, ambas tendrán SID diferentes. Esto asegura que ninguna cuenta de usuario reciba accidentalmente permisos originalmente asignados a otro usuario con el mismo nombre.

Para mantener las cuentas de usuario, se debe utilizar la consola de administración de Usuarios y computadoras del directorio activo (AD). Si usted quiere abrir esta consola haga clic en el menú Start, seleccione Programs y, después, seleccione Administrative Tools. Una vez que esté

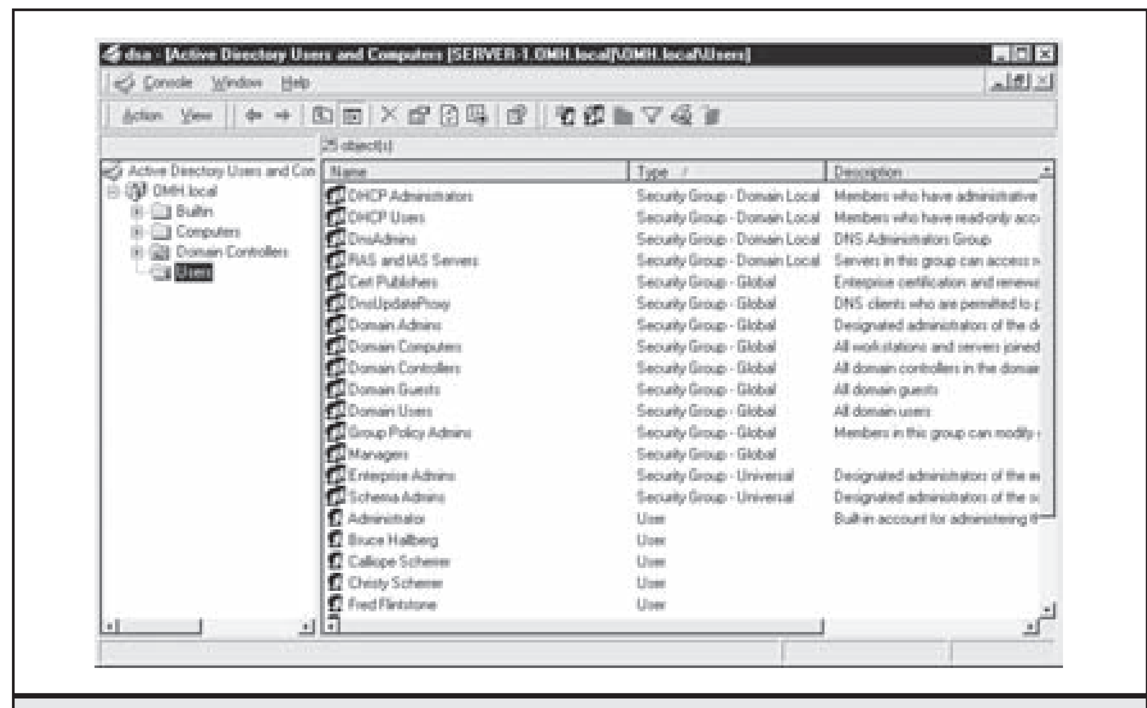


Figura 17-1. Consola Active Directory Users and Computers.

abierta la consola, abra el árbol del dominio que usted administra y, después, haga clic sobre el fólder Users. Su pantalla deberá verse de forma muy similar a la que se muestra en la figura 17-1 en este punto.

Para realizar actividades en la consola, debe seleccionar ya sea un contenedor en el lado izquierdo o un objeto en el lado derecho de la ventana y, después, ya sea hacer clic con el botón derecho del mouse en el contenedor o el objeto o abrir el menú Action y seleccionar alguna de las opciones disponibles. Debido a que las opciones disponibles cambian según sea el contenedor u objeto seleccionados, seleccione primero un objeto con el cual trabajar es importante.

Adición de un usuario

Para agregar un usuario mediante la consola AD Users and Computers, comience seleccionando el contenedor Users en el lado izquierdo (con el árbol abierto en el dominio que usted está administrando). Después, con el botón derecho haga clic en el contenedor Users, seleccione New del menú y después seleccione la opción User del submenú. Usted verá la caja de diálogo Create New Object (User) que se muestra en la figura 17-2.

Llene los campos First Name, Last Name y User Logon Name. Después, haga clic en el botón Next para moverse a la siguiente caja de diálogo, la cual se muestra en la figura 17-3.

Figura 17-2. Utilice la caja de diálogo Create New Object (User) para agregar un nuevo usuario.

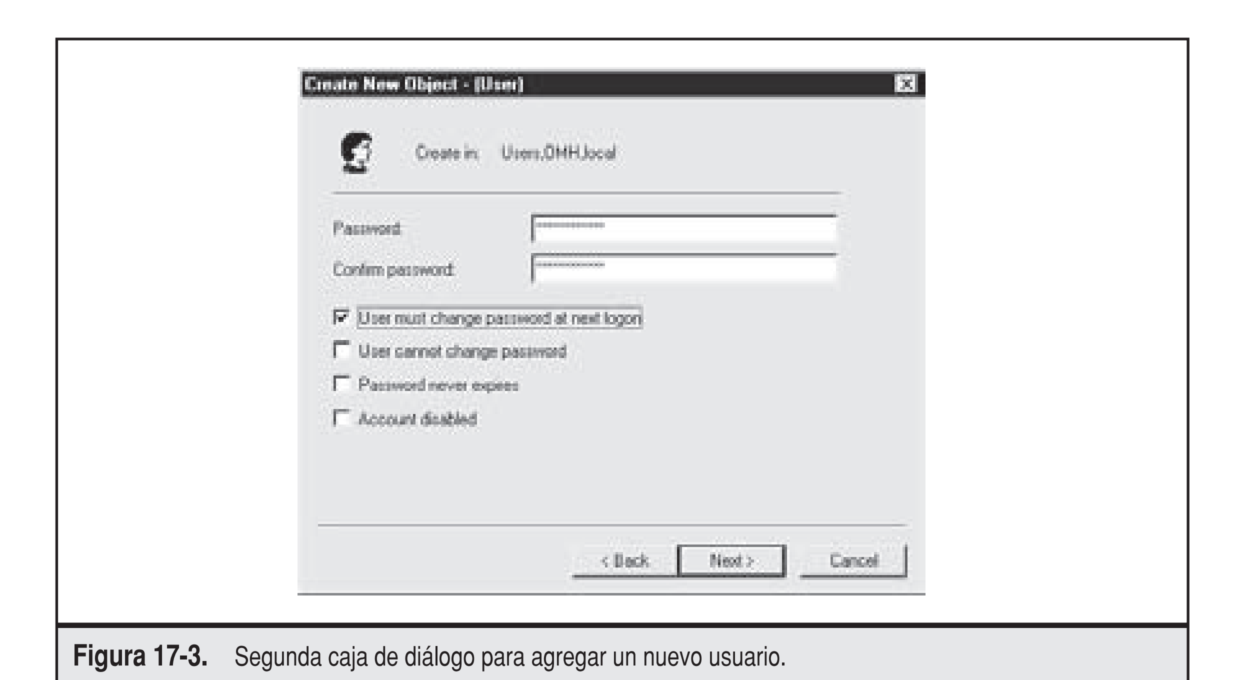


Figura 17-3. Segunda caja de diálogo para agregar un nuevo usuario.

NOTA Usted debe establecer estándares por medio de los cuales pueda asignar nombres de acceso a su red. Las redes pequeñas (aquellas con menos de 50 usuarios) a menudo utilizan solo los nombres propios de las personas, seguidos de la primera inicial de sus apellidos cuando se presenta un conflicto. Una convención que se emplea con frecuencia es utilizar el apellido del usuario seguido de la primera inicial de su nombre propio. Este último permite un número mucho mayor de combinaciones antes de que se presente un conflicto y usted podrá resolver cualquiera que se le presente mediante la adición de la inicial de en medio de la persona, un número o cualquier otro cambio a fin de que los nombres de todos los usuarios en el sistema sean únicos en todo momento.

En la segunda caja de diálogo ingrese la contraseña inicial que utilizará la cuenta. También seleccione algunas de las siguientes opciones que se aplicarán:

- **User Must Change Password at Next Logon** La selección de esta caja de verificación obliga a los usuarios a seleccionar su propia contraseña cuando ingresen al sistema por primera vez.
- **User Cannot Change Password** Puede seleccionar esta opción para cuentas de recursos si no desea permitirles a los usuarios que cambien su contraseña. Sin embargo, en general, usted no deberá seleccionar esta opción; en la mayoría de los sitios se les permite a los usuarios cambiar sus contraseñas y querrá permitirles hacer lo mismo si ha configurado el sistema también para que las contraseñas expiren automáticamente.
- **Password Never Expires** Seleccione esta opción para permitir que la contraseña permanezca válida por el tiempo que el usuario quiera utilizarla. La activación de esta opción para todos los usuarios se considera, en general, una práctica de seguridad pobre, por lo que deberá considerar con mucho cuidado si desea habilitar esta opción.
- **Account Disabled** La selección de esta opción inhabilita la nueva cuenta. El administrador puede habilitar la cuenta cuando sea necesario quitando la marca en esta opción.

Después de ingresar la contraseña y seleccionar las opciones que desee, para continuar haga clic en Next. A renglón seguido usted verá una pantalla de confirmación. Haga clic en Next una vez más para crear la cuenta o clic en Back para regresar y hacer cualquier cambio necesario.

Modificación de una cuenta de usuario

Las cajas de diálogo que ve cuando crea una cuenta de usuario son mucho más sencillas que la que ve cuando la modifica. La caja de diálogo en la que modifica la información acerca del usuario contiene otros campos que puede utilizar para documentar la cuenta y configurar otras opciones de seguridad.

Para modificar una cuenta de usuario, haga clic con el botón derecho del mouse en el objeto del usuario que desea modificar y seleccione Properties del menú. Usted podrá ver a continuación la caja de diálogo con pestañas que se muestra en la figura 17-4.

En las primeras dos pestañas, General y Address, usted podrá ingresar información adicional acerca del usuario, como su título, dirección, número telefónico, cuenta de correo electrónico, etc. Debido a que Active Directory también se integra con las nuevas versiones de Exchange Server, esta información puede ser muy importante para su red.

Figura 17-4. Caja de diálogo Properties de un usuario.

La tercera pestaña, Account, que se muestra en la figura 17-5, es donde puede fijar algunas opciones importantes en la cuenta del usuario.

La primera línea de la caja de diálogo define el nombre de ingreso a Windows 2000 del usuario, así como el dominio de Windows 2000 en el que el usuario tiene membresía principal. La segunda línea define el nombre de ingreso a Windows NT del usuario, el cual éste puede utilizar opcionalmente si necesita ingresar al dominio desde una computadora con Windows NT o utilizar una aplicación que todavía no soporte los ingresos al Active Directory. (Aunque usted pueda establecer estos dos nombres de acceso para que sean diferentes, hacerlo raras veces es una buena idea).

Si hace clic en el botón Logon Hours se despliega la caja de diálogo que se muestra en la figura 17-6. En ella, usted puede seleccionar diferentes bloques de tiempo dentro de una semana estándar y, después, hacer clic en el botón de la opción adecuada para permitir o negar el acceso a la red en ese periodo. En la figura 17-6, los parámetros solo permiten tiempos de ingreso en horas de trabajo normal, con alguna tolerancia antes y después de esas horas a fin de dar cabida a horas de trabajo normal ligeramente diferentes. Por omisión, a los usuarios se les permite ingresar a la red a cualquier hora, cualquier día de la semana. En la mayoría de las redes, particularmente en las pequeñas, es aceptable permitir a los usuarios el acceso en cualquier momento.

Figura 17-5. Pestaña Account de la caja de diálogo Properties de un usuario.

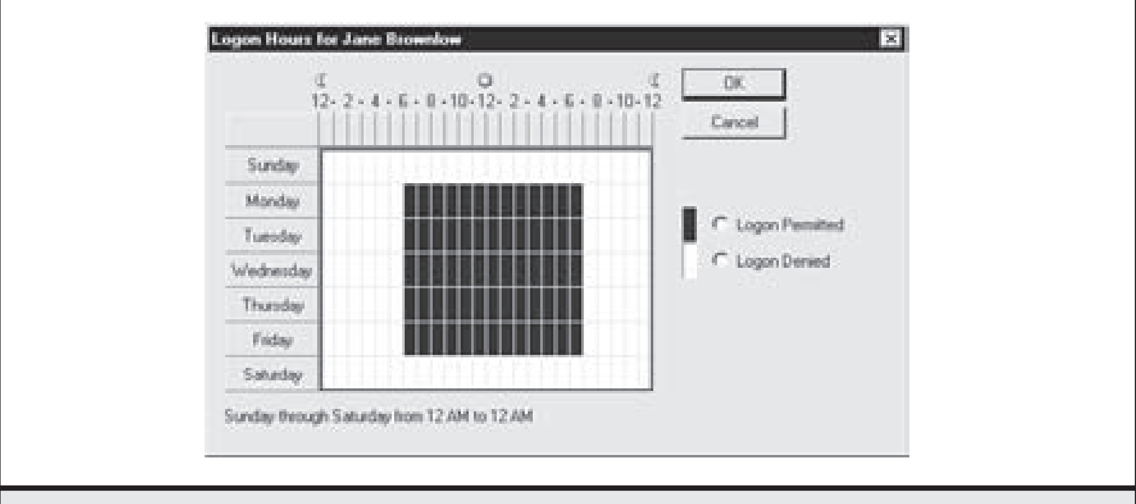


Figura 17-6. Configuración de las restricciones de tiempo de ingreso a la red de un usuario.

Otro botón en la pestaña Account de la caja de diálogo Properties del usuario (vea la figura 17-5) es el botón Logon To, el cual abre la caja Logon Workstations que se muestra en la figura 17-7. Por omisión, los usuarios pueden ingresar a cualquier estación de trabajo del dominio y éste los autentificará. En algunos casos, el sistema podrá requerir una seguridad más estricta, donde usted deberá especificar las computadoras a las que podrá tener acceso un usuario. Por ejemplo, podrá configurar una cuenta de respaldo de la red para utilizarla y después dejar esta cuenta firmada todo el tiempo en su cuarto de computadoras cerrado con llave. Debido a que la cuenta de respaldo tiene acceso a todos los archivos de la red (o no podría hacer su trabajo), una buena idea es limitar esa cuenta para que solo pueda acceder a la red desde la computadora designada para este propósito en el cuarto de computadoras. Se debe utilizar el botón Logon To para establecer este tipo de restricciones.

NOTA La facilidad Logon To funciona solo si la red utiliza los protocolos NetBIOS o NetBEUI. Esta facilidad no funcionará con redes que tengan solamente TCP/IP, a menos que se configure el servicio WINS en la red.

Usted debe estar consciente de que permitir que un usuario llamado George (por ejemplo) ingrese a la computadora de otro usuario no significa que George pueda ingresar con permisos del otro usuario o acceder a todo lo que este último pueda acceder. Esto significa simplemente que George puede utilizar la computadora física listada para acceder a su propia cuenta desde esa computadora.

La sección Account Options de la pestaña Account le permite seleccionar varias opciones binarias (Encendido/Apagado) de la cuenta, como requerir que un usuario modifique su contraseña la siguiente vez que ingrese, las establece conforme se agrega la cuenta. Algunas de las opciones que se presentan son únicas de la caja de diálogo Properties del usuario. Las dos más importantes de estas opciones adicionales son Account Is Disabled y Account Is Trusted for Delegation. Si se selecciona Account Is Disabled, se inhabilita la cuenta del usuario mientras que se deja habilitada dentro del Directorio activo. Esta opción es útil si usted necesita negar el acceso

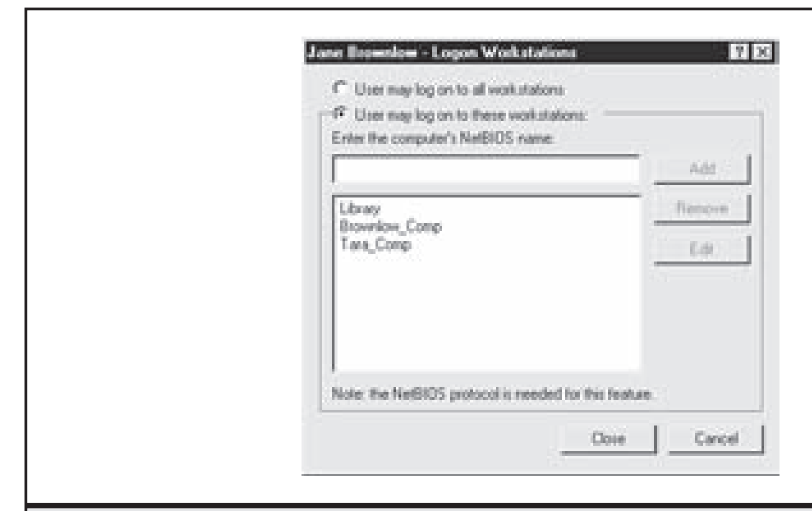


Figura 17-7. Restricción de las computadoras a las que puede ingresar un usuario.

a la red pero necesita habilitar la cuenta otra vez en el futuro. (Asimismo, Account Is Disabled se maneja como un cambio de alta prioridad dentro del dominio, y toma efecto inmediatamente, aun entre un gran número de controladores de dominio). Debido a que la eliminación de una cuenta también elimina cualquier permiso que el usuario pueda tener, usted deberá siempre inhabilitar la cuenta si necesita otorgar acceso a la red a ese usuario. (Por ejemplo, si alguna persona está de vacaciones, usted podría inhabilitar la cuenta de usuario mientras éste estuviera ausente y después quitar la marca en la opción Account Is Disabled cuando él regrese a trabajar). Usted deberá seleccionar la segunda opción, Account Is Trusted for Delegation, si desea designar la cuenta de usuario para administrar alguna parte del dominio. Windows 2000 Server le permite otorgar derechos administrativos a porciones del árbol Directorio activo sin tener que otorgar derechos administrativos a todo el dominio.

La última opción en la pestaña Account de la caja de diálogo Properties del usuario es para establecer la fecha de expiración, Account Expires. Por omisión, está fijada a Never. Si desea definir una fecha de expiración, lo puede hacer en el campo End Of. Cuando se llega a la fecha indicada, la cuenta se inhabilita automáticamente (sin embargo, no se elimina, a fin de que pueda habilitarla de nuevo si así lo desea).

Otra pestaña que utilizará con mucha frecuencia en la caja de diálogo Properties del usuario es la pestaña Member Of, en la que usted define los grupos de seguridad de un usuario. La figura 17-8 muestra esta pestaña. Los grupos de seguridad se estudian más adelante en este capítulo.

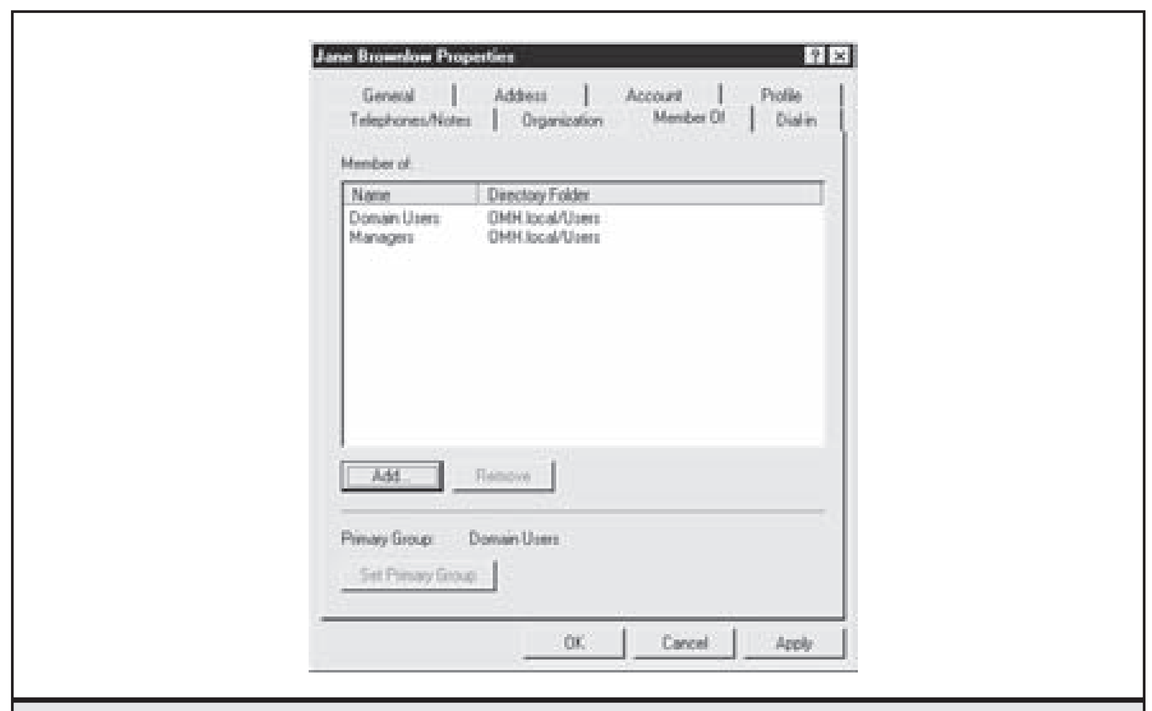


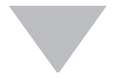
Figura 17-8. Control en grupos de la calidad de miembro de un usuario.



Eliminación o inhabilitación de una cuenta de usuario

Es fácil eliminar una cuenta de usuario utilizando la consola de Active Directory and Groups Management. Utilice el lado izquierdo para seleccionar el fólder Users y, después, seleccione el usuario en el lado derecho. Luego, haga clic con el botón derecho del mouse sobre el usuario y seleccione Delete, o abra el menú Action y seleccione Delete.

Es igual de sencillo inhabilitar una cuenta. Como antes, primero seleccione la cuenta del usuario. Después, haga clic con el botón derecho en ella y seleccione Disable Account o abra el menú Action y seleccione Disable Account.



PISTA Si usted necesita eliminar un gran número de cuentas, puede ahorrar tiempo seleccionándolas a todas antes de escoger los comandos Delete o Disable Account. ¡Sólo asegúrese de que no haya seleccionado cuentas que no quiera eliminar o inhabilitar!

TRABAJO CON GRUPOS DE SEGURIDAD WINDOWS 2000

En cualquier red, usted generalmente tendrá que administrar permisos a muchos fólders y archivos diferentes. Si solo pudiera otorgar acceso por cuenta de usuario, se volvería loco rápidamente si tuviese que llevar un registro por escrito de toda la información necesaria. Por ejemplo, suponga que un grupo de personas, como el departamento de contabilidad, tuviera diferentes permisos para acceder a 20 diferentes fólders en el servidor. Cuando se contrate un nuevo contador, ¿tendrá que recordar o consultar qué tienen esos 20 fólders, a fin de que pueda proporcionar al contador los mismos permisos que al resto de su departamento? O suponga que un usuario que tenga muchos permisos diferentes cambie de departamento. ¿Será necesario que usted tuviera que encontrar cada permiso que el usuario tenga a fin de asegurarse de que tiene solamente los adecuados para su nuevo departamento?

Para resolver dichos problemas, todos los sistemas operativos de red soportan el concepto de *grupos de seguridad* (o solamente *grupos*). Usted primero crea dicho grupo y después asigna a él todos los usuarios adecuados a fin de que pueda administrar sus permisos más fácilmente. Cuando otorga permiso a un fólder en un servidor, lo hace dando al grupo el permiso de la red. Todos los miembros del grupo *heredan* automáticamente dichos permisos. Esta herencia hace más fácil que se conserven los permisos de la red a través del tiempo. De hecho, usted no debe tratar de administrar los permisos de la red sin utilizar los grupos de esta forma. Rápidamente se verá saturado si trata de mantener un registro por escrito de todo, y es muy probable que, con el tiempo, cometa muchos errores.

Los usuarios no solo podrán ser miembros de grupos, sino que éstos pueden ser miembros de otros grupos. De esta forma, usted puede construir una jerarquía de grupos que haga aún más fácil su administración. Por ejemplo, suponga que usted define un grupo para cada departamento de su compañía. La mitad de dichos departamentos son parte de una división más grande llamada Investigación y desarrollo (R&D) y la otra mitad es parte de Ventas y administración general (SG&A). En su red, algunos fólders son específicos de cada departamento, otros lo son de todos los de R&D o SG&A y a otros más se puede accesar por cualquier usuario de la red. En dicha situación, usted podría crear los grupos departamentales y, después, crear los grupos R&D

y SG&A. Cada grupo podría, entonces, convertirse en un miembro ya sea de R&D o SG&A. Por último, usted podría utilizar el grupo Domain Users incluido, u otro que haya creado que represente a todos y, después, asignar a R&D y SG&A ese grupo de alto nivel a cada usuario.

Una vez que haya hecho estos agrupamientos, podrá otorgar permisos de una manera lógica. Si un recurso es solo de un departamento específico, se lo debe asignar a ese grupo departamental. Si un recurso es de R&D o SG&A, se lo asigna a esas divisiones; después, todos los grupos departamentales que conforman esa división heredarán permiso para acceder a ese recurso. Si un recurso es para todos, usted podría asignarlo al grupo master de alto nivel. El empleo de dichos niveles jerárquicos de grupos facilita de manera notable la administración de permisos y es prácticamente indispensable para redes más grandes que cuenten con cientos de usuarios.

Creación de grupos

Usted puede crear grupos mediante el empleo de la misma consola que usa para los usuarios: la Active Directory Users and Computers. Los grupos aparecen en dos de los contenedores de dominio: Built-In y Users. Los grupos Built-In tienen ciertos permisos importantes ya asignados y los otros grupos que cree pueden ser incorporados a ellos. De manera similar, si usted desea inhabilitar un grupo Built-In en particular, puede hacerlo simplemente quitando todos sus grupos miembros. La figura 17-9 muestra la lista de grupos Built-In de Windows 2000 Server.

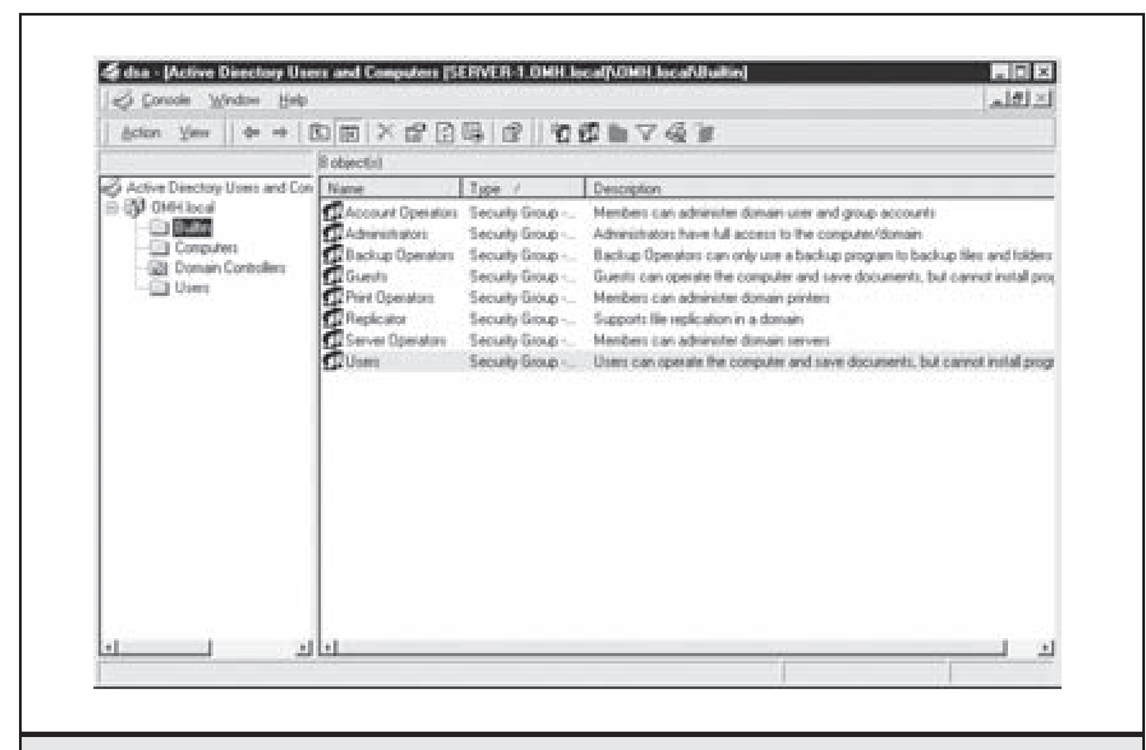
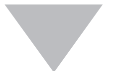


Figura 17-9. Lista de grupos incluidos.



PRECAUCIÓN Sea especialmente cuidadoso al cambiar los miembros de los grupos incluidos. En la mayoría de las redes, mientras se comprende qué son estos grupos y cómo trabajan, es mejor no tocarlos.

En general, usted solo trabaja con grupos definidos en el contenedor Users. La figura 17-10 muestra los grupos por omisión en el contenedor Users, el cual puede diferenciar de las cuentas de usuarios por el icono de las dos personas y por la designación Type.

Para agregar un nuevo grupo, primero seleccione el contenedor Users del lado izquierdo de la ventana. Después, abra el menú Action, seleccione New y después Group. Usted podrá ver la caja de diálogo Create New Object (Group) que se muestra en la figura 17-11.

Primero ingrese el nombre del grupo en el campo que se proporciona. Usted podrá observar el nombre que ingresó repetido en el campo Downlevel Name of New Group. Este campo le permitirá especificar un nombre de grupo diferente para computadoras con Windows NT. Sin embargo, utilizar diferentes nombres de grupo no es, en general, una buena idea ya que su sistema puede hacerse muy confuso rápidamente.

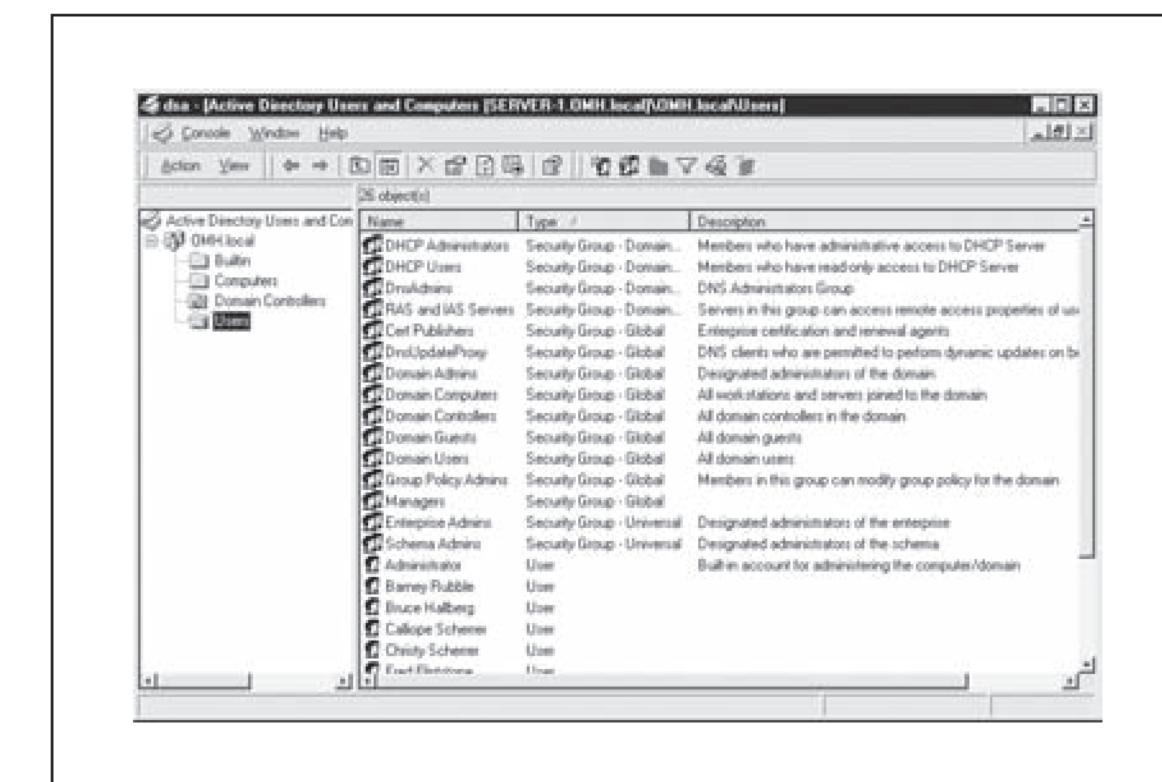


Figura 17-10. Grupos por omisión del contenedor Users.

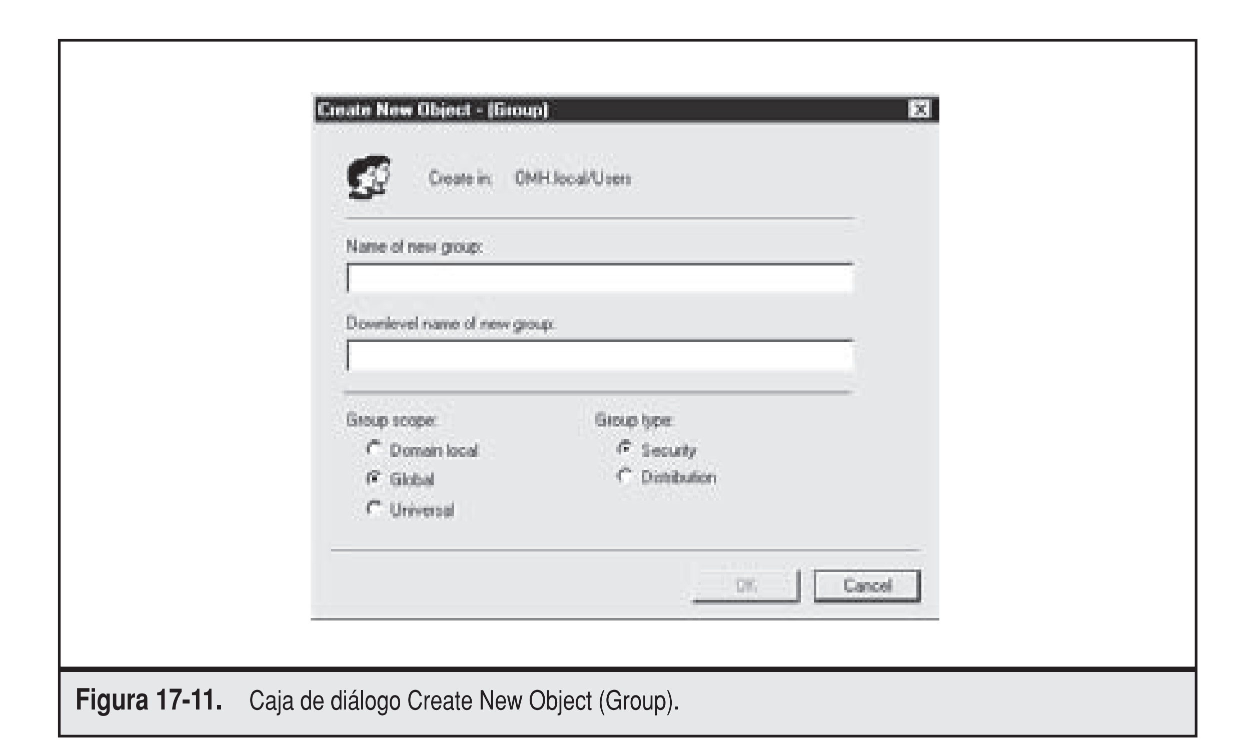


Figura 17-11. Caja de diálogo Create New Object (Group).

Después de asignarle un nombre al grupo, usted necesita seleccionar algunos de los botones de opción disponibles en la mitad inferior de la caja de diálogo. El Group Scope se refiere a qué tan poblado está el grupo dentro de un dominio. Existe un *grupo universal* que abarca toda una organización, aun cuando la red de la misma esté conformada por muchos dominios individuales. Además, los grupos universales pueden también contener miembros de cualquier dominio en la red de una organización. Por otro lado, un grupo global solo puede contener miembros del dominio en el que existe. Sin embargo, usted puede asignar permisos de grupos globales a cualquier dominio dentro de la red, incluso entre múltiples dominios. Por último, los *grupos locales de dominio* existen solamente dentro un solo dominio y únicamente pueden contener miembros de ese dominio.

PISTA No se preocupe si usted crea un grupo con un alcance equivocado, pues éste se puede cambiar fácilmente, siempre y cuando la membresía no viole sus nuevas reglas de alcance. Para modificar el alcance del dominio, seleccione el grupo y abra su caja de diálogo Properties (haga clic con el botón derecho del mouse y después seleccione Properties del menú). Si la membresía de grupo permite el cambio, usted puede seleccionar un botón de opción diferente en el Grupo Scope.

Después de que haya establecido el alcance del grupo, también puede seleccionar si éste será un *grupo Security* o un *Distribution*. Estos últimos se utilizan solamente para mantener las listas de distribución de correo electrónico y no tienen efecto en la seguridad de Windows 2000 Server. Se emplean solamente en aplicaciones de correo electrónico, como Microsoft Exchange Server.



Mantenimiento de los miembros de los grupos

Después de que usted haya terminado de llenar las opciones de la caja de diálogo Create New Object (Group) y dado clic en OK, el programa crea un nuevo grupo, pero éste comienza sin ningún miembro. Para establecer los integrantes de un grupo, siga los pasos siguientes:

1. Seleccione el grupo y abra su caja de diálogo Properties (para ellos, haga clic con el botón derecho del mouse y después seleccione Properties del menú).
2. Haga clic en la pestaña Members. Aparecerá la caja de diálogo Group Properties que se muestra en la figura 17-12.
3. Haga clic en el botón Add. Aparecerá la caja de diálogo Select Users, Contacts, Computers or Groups que se muestra en la figura 17-13.
4. Desplácese por la lista para seleccionar cada miembro que desea agregar al grupo, y después haga clic en el botón Add para agregar los que se seleccionaron a la lista de miembros. La lista desplegará solo objetos que puedan ser miembros del grupo.

Si desea ser un miembro del otro grupo, haga clic en la pestaña Member Of de la caja de diálogo Group Properties y después haga clic en su botón Add, de manera parecida a como agregó miembros al grupo.

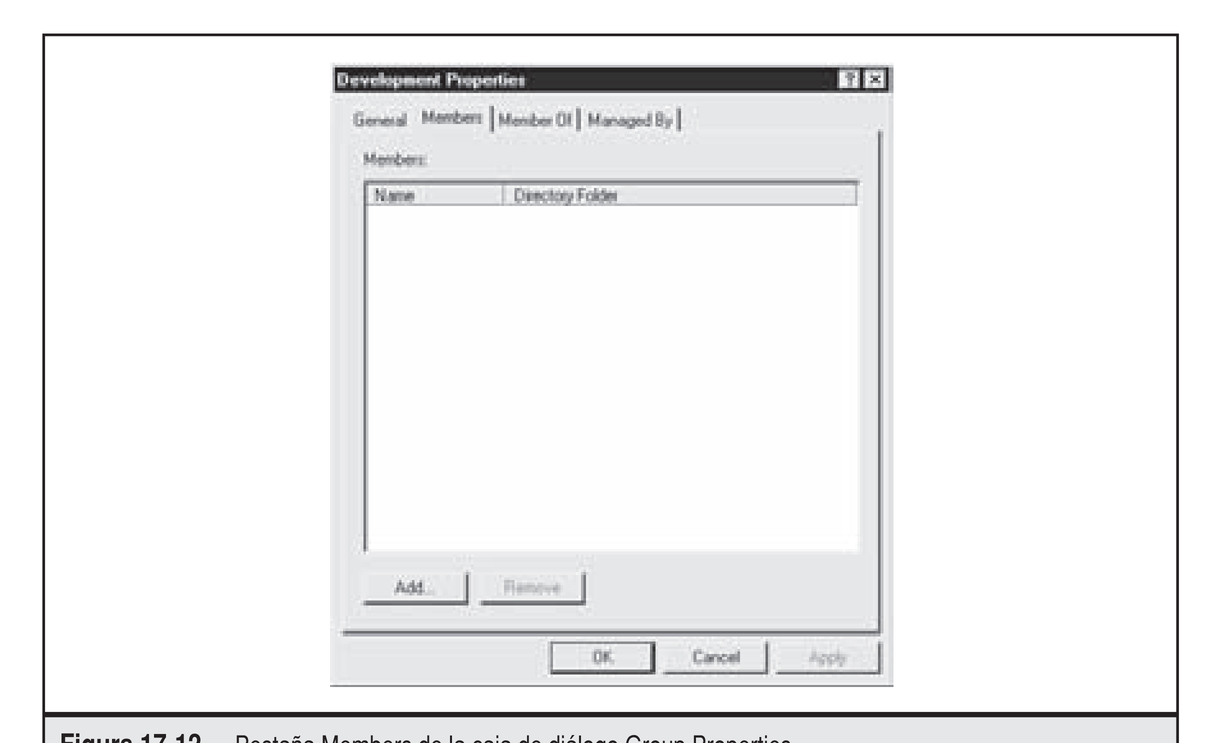


Figura 17-12. Pestaña Members de la caja de diálogo Group Properties.

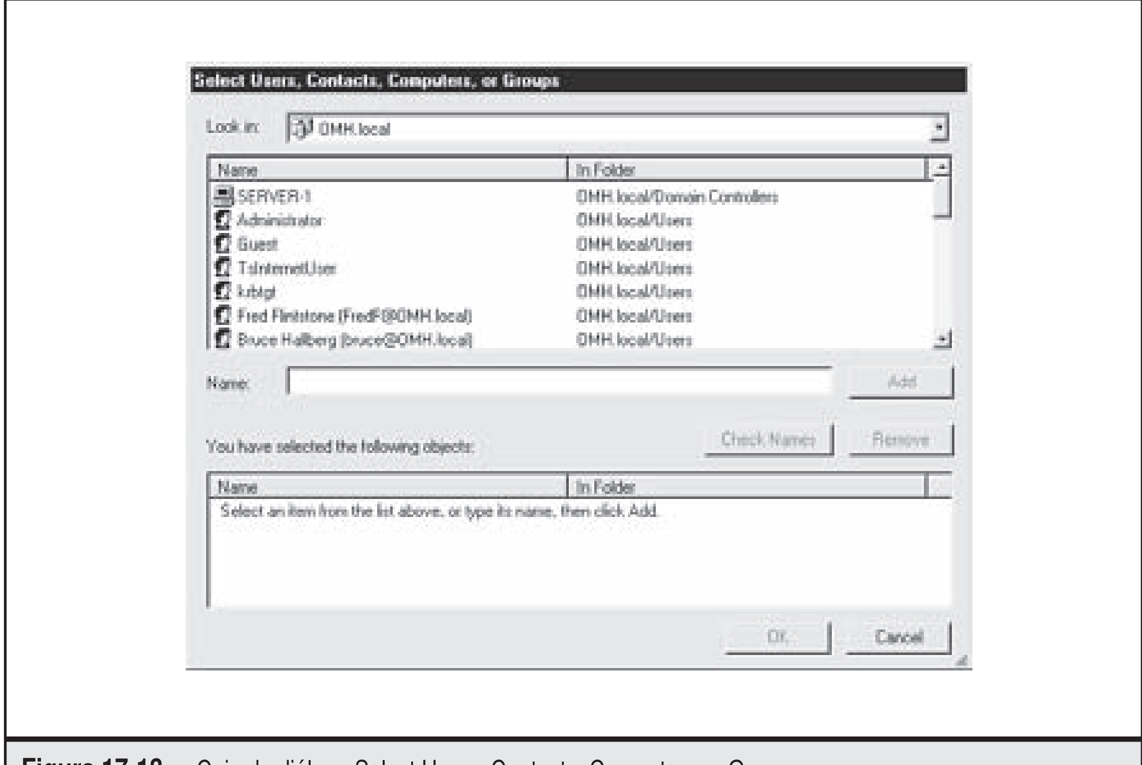


Figura 17-13. Caja de diálogo Select Users, Contacts, Computers or Groups.

TRABAJO CON COMPARTICIONES

Los controladores y fólders del ambiente de Windows 2000 Server se encuentran disponibles para los usuarios de la red como recursos compartidos, llamados simplemente *comparticiones* en el lenguaje de la conectividad de redes. Usted selecciona un controlador o fólder, permite que éste sea compartido y, después, establece los permisos de la compartición.

Comprensión de la seguriddad de la compartición

Usted puede establecer controladores como fólders o como recursos (o *comparticiones*) compartidos distintos, ya sea que estén ubicados en controladores formateados como FAT o como NTFS. Sin embargo, solo en el caso de un controlador formateado como NTFS usted puede también establecer permisos en fólders y archivos dentro de la compartición que esté separada de los permisos en la misma. Comprender la forma en que Windows 2000 maneja la seguridad de las comparticiones, fólders y archivos en los controladores NTFS es importante.

Suponga que crea una compartición llamada RESEARCH y le otorga al grupo de seguridad R&D acceso de solo lectura. Dentro de ella, usted establece los permisos en un fólder llamado

PROJECTS a fin de permitir acceso total a lectura y escritura (llamado *Change permission*) al grupo de seguridad R&D. La pregunta es: ¿tendrá el grupo de R&D permiso de solo lectura a este fólder o permiso de cambio? La respuesta es que el grupo tendrá permiso de solo lectura ya que cuando los permisos de seguridad difieren entre fólders dentro de una compartición y en la compartición misma, se aplican los permisos más restrictivos. Una mejor forma de establecer estos permisos, es permitir a todos permiso de cambio (Change permission) a la compartición y, después, controlar los permisos actuales colocándolos en los fólders dentro de la compartición misma. De esta forma, usted puede asignar cualquier combinación de permisos que desee; entonces, los usuarios recibirán los que usted estableció en esos fólders, a pesar de que la compartición está fijada a permiso de cambio.

Recuerde que los usuarios reciben los permisos con base en los grupos de los que son miembros, y que estos permisos son acumulativos. Por tanto, si es un miembro del grupo Everyone y éste tiene permiso de solo lectura de un archivo en particular, pero usted es también miembro del grupo Admins que tiene permiso de control total de ese archivo, en la práctica tendrá permiso de control total. Ésta es una regla importante: los permisos que se colocan en fólders y archivos son siempre acumulativos y toman en cuenta los establecidos para el usuario individual así como cualquiera de los grupos de seguridad de los que el usuario sea miembro.

El siguiente aspecto a recordar es que usted puede establecer permisos dentro de una compartición (a menudo llamados *permisos NTFS*) en ambos fólders y archivos, los cuales también son acumulativos. Por lo que, por ejemplo, usted puede establecer para un usuario permiso de solo lectura con respecto a un fólder, pero otorgar permiso de cambio para algunos archivos específicos. En este caso, el usuario tendrá capacidad para leer, modificar y aun eliminar esos archivos, lo cual no sucede con los demás archivos de este mismo fólder.

El último aspecto a recordar es que existe un permiso especial llamado No acceso, que elimina a todos los demás permisos sin importar cuáles sean. Si establece el permiso de no acceso a un usuario en un archivo o fólder, entonces es eso: el usuario no tendrá acceso a ese archivo o fólder. Un corolario extremadamente importante a esta regla es que el permiso de no acceso también es acumulativo y superior a los demás. Por tanto, si el grupo de seguridad Todos tiene permiso para cambiar un archivo, pero usted fija a un usuario en particular el no acceso a ese archivo, éste usuario recibirá permiso de no acceso. Si establece permiso de no acceso al grupo Todos, todos los miembros de ese grupo también recibirán No acceso ya que éste es superior a cualquier otro permiso que tengan. ¡Sea cuidadoso en el uso de No acceso con los grupos de seguridad! Existen muchos otros puntos finos para establecer y mantener permisos que van más allá del alcance de este libro, pero puede resolver la mayoría de los problemas de permisos si recuerda las reglas que se estudian aquí:

- Cuando los permisos de compartición entran en conflicto con los permisos de archivo o de fólder, el permiso *más restrictivo* siempre gana.
- Además, los permisos son acumulativos, esto es, se toman en cuenta los permisos asignados a los usuarios y grupos así como los archivos y fólders.
- Cuando se presenta un permiso en conflicto, el permiso de No acceso siempre gana.

CREACIÓN DE COMPARTICIONES

Como administrador de la red, usted tendrá que crear y administrar las comparticiones (recursos compartidos) en la red con mucha frecuencia. Los pasos siguientes lo guiarán para crear una nueva compartición.

1. Utilice en el servidor My Computer o Windows Explorer.
2. Haga clic con el botón derecho del mouse sobre el fólder o controlador que desee compartir y, después, seleccione Sharing. Usted verá la pestaña Sharing del fólder o la caja de diálogo Properties del controlador, como se muestra en la figura 17-14.
3. Haga clic en el botón de opción Share this folder, después asigne un nombre de compartición y, si lo desea, agregue un comentario respecto a la misma. (Los usuarios podrán ver el comentario que usted haga). Después de asignarle un nombre, puede seleccionar un límite respecto de cuántos usuarios pueden acceder de manera simultánea. (Normalmente, deje la opción User Limit fijada en Maximum Allowed).
4. El último paso es verificar los permisos de la compartición.

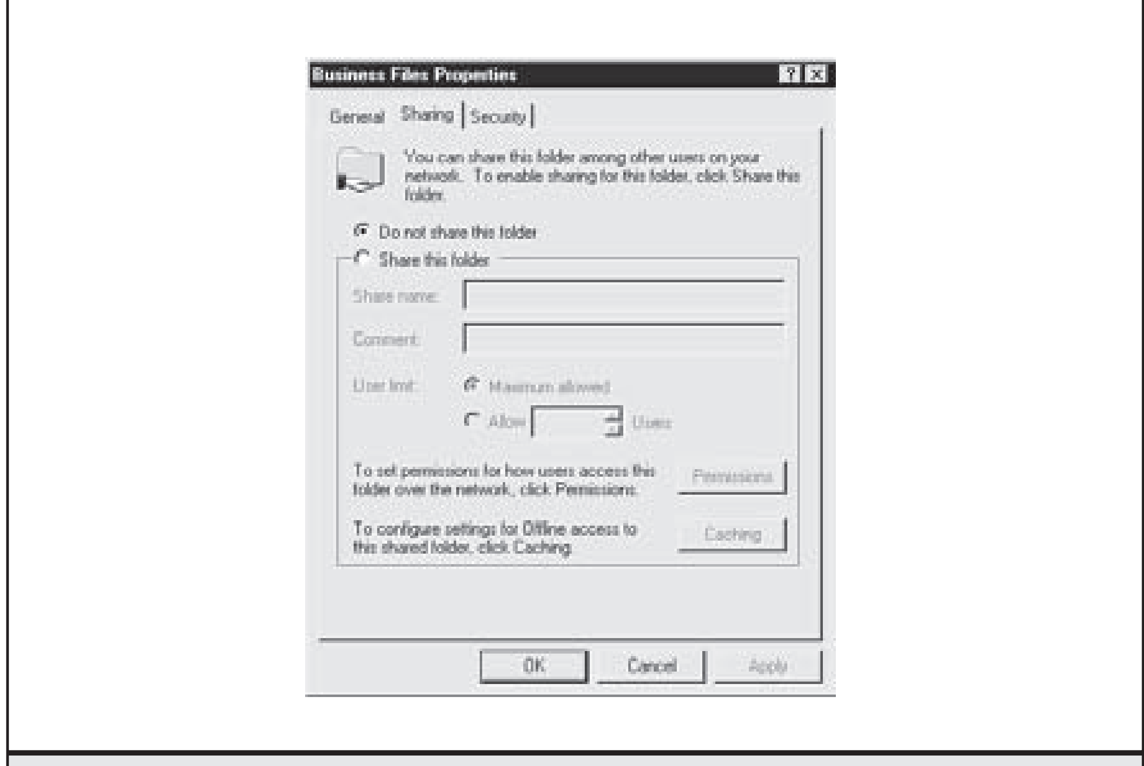


Figura 17-14. Pestaña Sharing de la caja de diálogo Properties de un fólder.

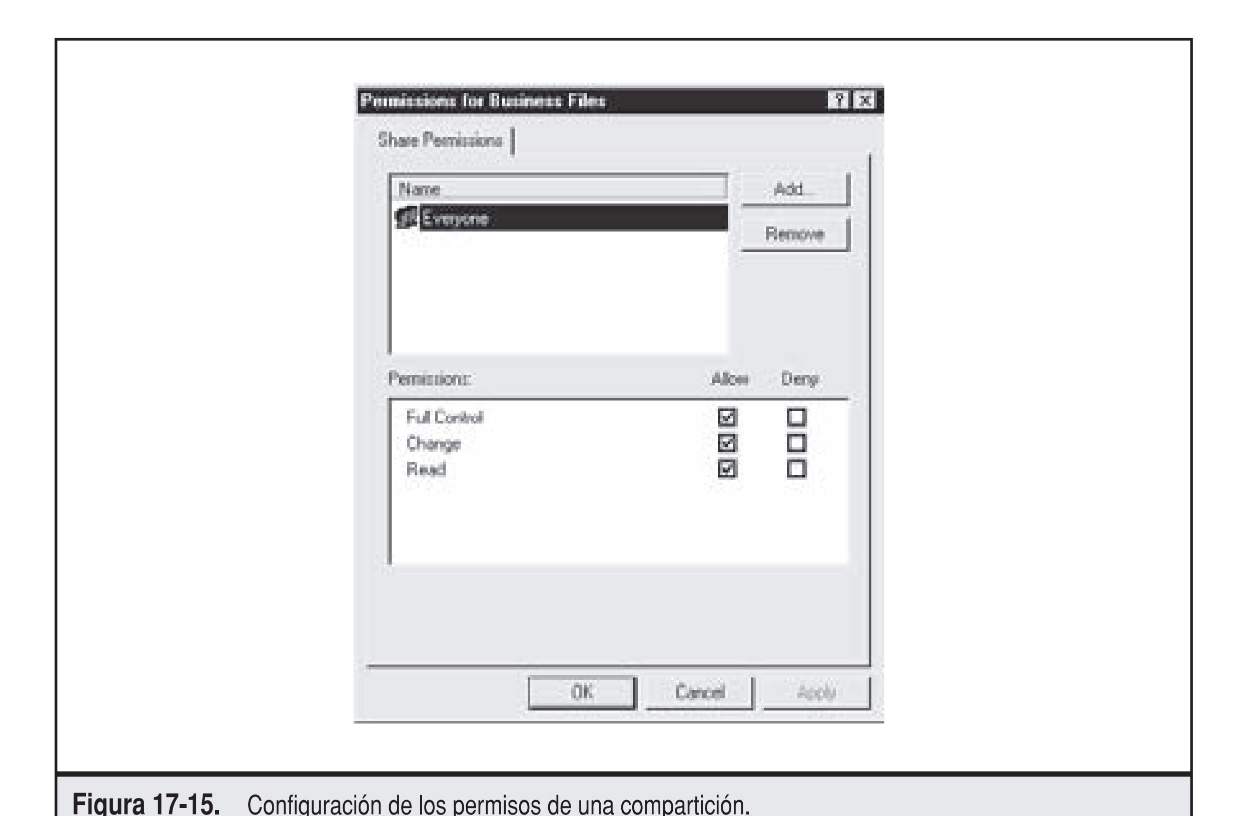


Figura 17-15. Configuración de los permisos de una compartición.

5. Haga clic en el botón Permissions, el cual despliega la caja de diálogo Permissions que se muestra en la figura 17-15. Como puede observar, el parámetro por omisión de una compartición es que el grupo Everyone tenga el acceso más completo posible a ella. Normalmente, este parámetro es lo que usted desea. (Vea el análisis de la sección anterior acerca de los permisos de compartición para obtener más información acerca de este parámetro). Aun así, si necesita restringir de alguna manera el acceso, la caja de diálogo Permissions le permite hacerlo. Haga clic sobre Add y accederá a la caja de diálogo Select Users, Contacts, Computers o Groups, desde donde podrá seleccionar esas entidades y asignarles los permisos.
6. Después de agregar una entidad, puede utilizar las cajas de opción de la ventana Permissions de la caja de diálogo del mismo nombre para fijar exactamente los permisos que usted desee.
7. Cierre todas las cajas de diálogo activas utilizando el botón OK en cada una.

NOTA Cuando usted haga clic en una entidad y algunas de sus cajas de opción dentro de la caja de diálogo Permissions se pongan de color gris, significa que los permisos fueron heredados de un nivel superior, generalmente de los permisos establecidos en un fólder contenedor ubicado en algún lugar del árbol de directorios.

Una vez que se crea una compartición y la información compartida se propaga por el dominio (generalmente en cuestión de minutos), los usuarios pueden navegar en ella por medio de Network Neighborhood (Windows 9x y NT) o My Network Places (Windows 2000 y XP). Según los permisos, la podrá abrir si hace doble clic en compartición.

Usted puede esconder una compartición, pero mantenerla disponible para los usuarios que conozcan el nombre de la misma. Para hacerlo, creela normalmente, pero agregue el signo de dólar ($) al final de su nombre. Por ejemplo, FILE$ podría ser una compartición que los usuarios no puedan ver cuando estén navegando a través de la red.

Exploración de los controladores

Usted puede utilizar las comparticiones abriéndolas en Network Neighborhood o My Network Places, las que funcionan igual que los fólders en My Computer. Sin embargo, con frecuencia, deberá simular un disco duro conectado en su computadora con una compartición desde la red. Por ejemplo, muchas aplicaciones que almacenan archivos requieren que los fólders de red estén accesibles como letras de controlador normales. El proceso de simular un controlador de disco con una compartición de red se llama *exploración*, mediante la cual puede crear un mapa (enlace) entre la letra del controlador que desea utilizar y la compartición de red real que se mantendrá conectada a la letra del controlador.

Puede crear una exploración en un controlador de muchas maneras. La forma más fácil es abrir Network Neighborhood de la computadora cliente y, después, localizar la compartición que desee explorar. Haga clic con el botón derecho del mouse sobre él y seleccione Map Network Drive. En la caja de diálogo que se desplegará, aparecerán el nombre del dominio y la compartición ya tecleadas por usted; simplemente seleccione una letra de controlador apropiada para la exploración y haga clic en OK. De ahí en adelante, la compartición aparecerá en su computadora con esa letra de controlador y los usuarios la verán en My Computer.

Para conectar una compartición oculta, haga clic con el botón derecho del mouse en Network Neighborhood (o My Network Places for Windows 2000/XP) y seleccione Map Network Drive. Elija una letra de controlador para explorar, ingrese el nombre completo de la compartición (con el signo de dólar al final), y después haga clic en OK. Siempre y cuando tenga permiso para acceder a ésta, la exploración trabajará normalmente.

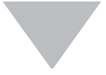
Usted puede también explorar controladores mediante el empleo de una utilidad de línea de comandos llamada NET. El *comando NET* toma muchas formas diferentes y puede satisfacer muchas necesidades, de acuerdo con los parámetros que le proporcione. Para explorar un controlador, utilice el comando NET USE. Teclee **NET USE** y luego presione ENTER, después de lo cual aparecerá una lista con todos los controladores explorados actualmente. Para agregar una nueva exploración de controlador, teclee lo siguiente:

NET USE *drive_letter:UNC_for_share*

La mayoría de los recursos de la red Windows utilizan un sistema denominativo llamado *Convención de nombrado universal (UNC)*. Para proporcionar una UNC, comience con dos diagonales invertidas, después el nombre del servidor, otra diagonal invertida y el nombre de la compartición. (Las diagonales invertidas y nombres adicionales se pueden referir a los fólderes y archivos incluidos en ésta). Por tanto, si desea explorar el controlador G: a una compartición llamada EMPLOYEES ubicada en el servidor SERVER, el comando podría ser como sigue:

NET USE G: \ \ SERVER \ EMPLOYEES





PISTA Usted puede utilizar el comando NET de cualquier cliente Windows para cualquier red Windows. Teclee **NET** para listar todas las diferentes formas del comando. Teclee **NET command HELP** para ver ayuda adicional sobre los diferentes comandos NET.

ADMINISTRACIÓN DE LAS COMPARTICIONES DE IMPRESORA

Antes de configurar y trabajar con impresoras en red, usted necesita comprender los componentes involucrados en la impresión de red y cómo interactúan entre sí, a saber:

- Un *trabajo de impresión* es un conjunto de datos binarios que se envían desde una estación de trabajo a una impresora de la red. Un trabajo de impresión son los mismos datos que una computadora enviaría a una impresora conectada localmente, pues solo se redirecciona a una red para su impresión.
- La estación de trabajo de la red que envía el trabajo a la cola de impresión es responsable de formatear adecuadamente los datos de impresión para la impresora. Esta tarea la hace por medio del software instalado en la estación de trabajo —llamado *controlador de impresión*— que es específico de cada tipo de impresora. Los controladores de impresión son también específicos de cada sistema operativo que los utiliza. En otras palabras, un controlador Hewlett-Packard LaserJet 5si de una computadora con Windows 95 es diferente de un controlador Hewlett-Packard LaserJet 5si de una computadora con Windows NT Workstation. Y el asunto es aún más problemático: por lo general, diferentes versiones del mismo sistema operativo utilizan distintos controladores, por lo que un controlador de una computadora con Windows 95 es probable que no funcione con una computadora Windows 98 y viceversa.
- A menudo, los trabajos de impresión se envían a la red a través de un puerto de impresión de captura. El software cliente de la red redirecciona a la red uno de los puertos de impresión de una estación de trabajo en red, como el LPT1. El proceso de redireccionar un puerto de impresión a una impresora de red se llama *captura*. En general, los puertos de captura son persistentes y se mantienen tratando de acceder a la impresora hasta que se apagan.
- Los trabajos de impresión que se envían a la red van a un lugar llamado *cola de impresión*. El trabajo de impresión se forma hasta que la red pueda dar servicio a ese trabajo y lo envíe a la impresora. Las colas de impresión pueden estar formadas por muchos trabajos de una gran cantidad de usuarios y, típicamente, se administran de acuerdo con el criterio de que el primero que entre será el primero en salir.
- Los trabajos de impresión se eliminan de las colas y se envían a las impresoras por medio de los *servidores de impresión*. Después de enviar el trabajo completo a la impresora, el servidor de impresión quita el trabajo de la cola. Usted puede llevar a cabo el servicio de impresión de muchas formas. Si la impresora que utiliza está conectada a un servidor o a una estación de trabajo de la red, entonces ese servidor o estación de trabajo administra la tarea del servidor de impresión. Si la impresora está conectada directamente a la red (si ésta tiene su propio puerto de red), por lo general cuenta con un

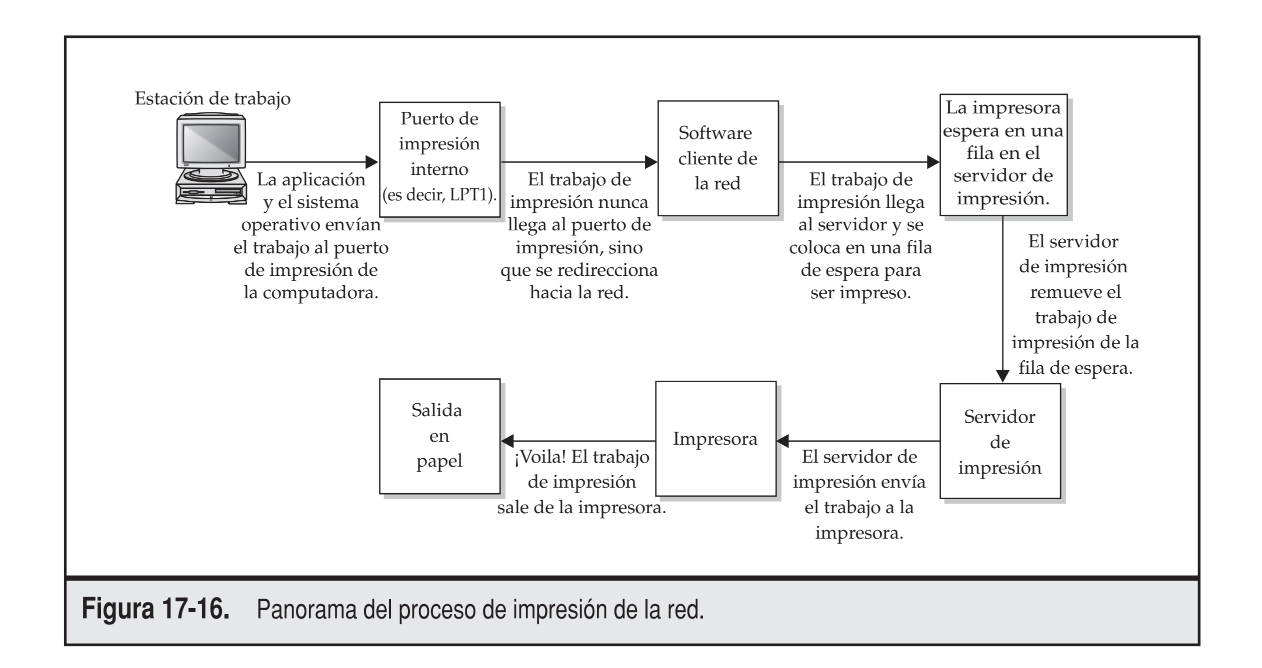


Figura 17-16. Panorama del proceso de impresión de la red.

servidor de impresión incorporado como parte de su hardware de red, el cual tiene inteligencia para acceder a la red y dar servicio a una cola de impresión en particular.

Los trabajos comienzan con la aplicación de impresión, la cual envía su salida al sistema operativo local. Éste utiliza el controlador de impresión solicitado por la aplicación para dar formato al trabajo de impresión para la impresora en cuestión. Después, trabaja con el software cliente de red instalado para enviar el trabajo de impresión formateado a la cola de impresión, donde el trabajo hace fila hasta que la impresora esté disponible. Posteriormente, el servidor de impresión envía el trabajo a la impresora. Muchos pasos están involucrados en este proceso, pero una vez que todo está configurado, funciona sin problemas, como usted lo podrá constatar en la siguiente sección. La figura 17-16 muestra un panorama de cómo funciona la impresión en la red.

CONFIGURACIÓN DE UNA IMPRESORA DE RED

Esta sección le enseña cómo configurar una impresora conectada directamente a un Windows 2000 Server que pondrá a disposición de los usuarios de la red. En este caso, la impresora y su controlador Windows 2000 ya están perfectamente instalados, como deberían estarlo normalmente durante la instalación del Windows 2000 Server. Si no están perfectamente instalados, entonces abra el fólder Printers y utilice el icono Add Printers para configurar la impresora en el servidor mismo.

Usted puede configurar fácilmente una impresora conectada a un servidor (o a una estación de trabajo), pero también otros usuarios de la red pueden acceder a ella. Sin embargo, en las redes con más de 20 usuarios, usted se sentirá más a gusto si compra impresoras con las interfases de

red y servidores de impresión incorporados o utiliza cajas de servidor de impresión, que sirvan de interfase entre una impresora y la red. Para la mayoría de las impresoras láser, agregar una interfase de red dedicada y un servidor incrementa el costo de la impresora en aproximadamente 300 dólares. Éste es dinero bien invertido ya que el envío de un trabajo de impresión a una impresora requiere que el servidor de impresión lleve a cabo un gran proceso. Si este servidor de impresión es también su servidor de archivos principal, su desempeño total disminuirá de manera significativa mientras imprime (y, en particular, mientras esté dando servicio a trabajos de impresión grandes). Asimismo, las impresoras que cuentan con servidores de impresión incorporados son mucho más fáciles de reubicar en la red, pues están en condiciones de ir a cualquier parte donde exista una conexión de red y donde esté disponible la alimentación. Una vez conectada a la red en un nuevo sitio, la impresora podrá acceder a ella y comenzar a hacer su trabajo inmediatamente.

Los pasos siguientes lo llevan por medio de la configuración de una impresora de red:

1. Para compartir una impresora conectada a Windows 2000 Server, primero abra el fólder Printers del servidor. (Abra el menú Start, seleccione Settings y después seleccione Printers). Usted verá todas las impresoras instaladas en el fólder Printers.

2. Haga clic con el botón derecho del mouse en la impresora que desee compartir y seleccione Sharing en el menú. Aparecerá la caja de diálogo Properties de la impresora, con la pestaña Sharing activada, como se muestra en la figura 17-17.

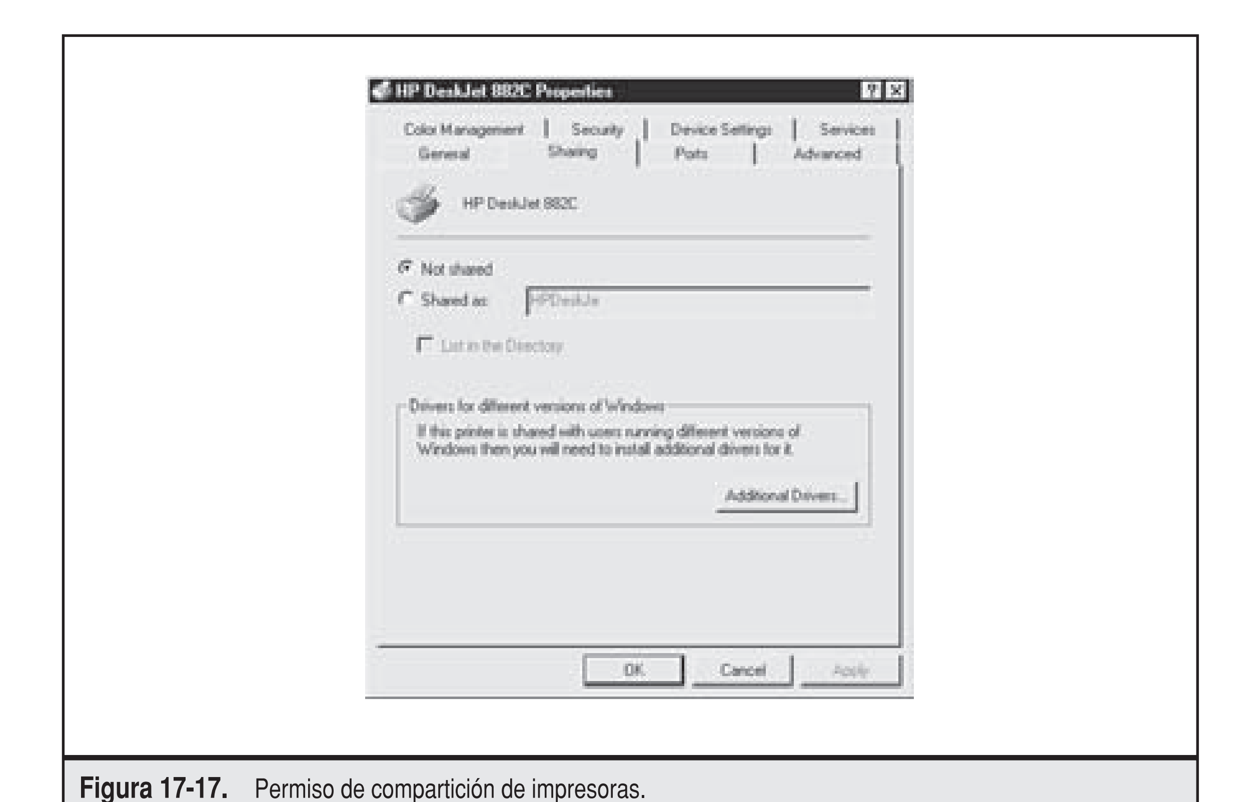


Figura 17-17. Permiso de compartición de impresoras.

3. Haga clic en el botón de opción Shared as y después asigne a la impresora un nombre compartido, por medio del cual las computadoras cliente reconocerán esa impresora. En este punto, usted puede hacer clic en el botón OK ya que los permisos por omisión para una impresora compartida son para que el grupo Everyone pueda imprimir en ella. En general, a pesar de eso, usted necesita verificar al menos dos de los demás parámetros disponibles, como sigue:

   - Para obtener altos niveles de desempeño, debe utilizar una herramienta llamada *pool de impresión*, la cual le permite configurar muchas impresoras idénticas, todas conectadas a una sola cola de impresión, que la red pueda ver como una sola impresora. Los usuarios imprimen en la impresora listada y la primera disponible proporciona el servicio. Por medio de la utilización del pool de impresión, usted puede tener todo un banco de impresoras que parezcan una sola para los usuarios y, dramáticamente, aumentar el número de solicitudes de impresión que pueda manejar. Sin embargo, recuerde que las impresoras poleadas deben ser idénticas ya que todas ellas utilizarán el mismo controlador de impresión. La figura 17-18 muestra la pestaña en la que se habilita el pool de impresión.
   - Para establecer los permisos para una impresora compartida, utilice la pestaña Security de la caja de diálogo Properties de la impresora, que se muestra en la figura 17-19. Los grupos que ve asignados en la figura son las asignaciones por omisión para una impresora compartida, que muestra los Administrators Permissions. Como

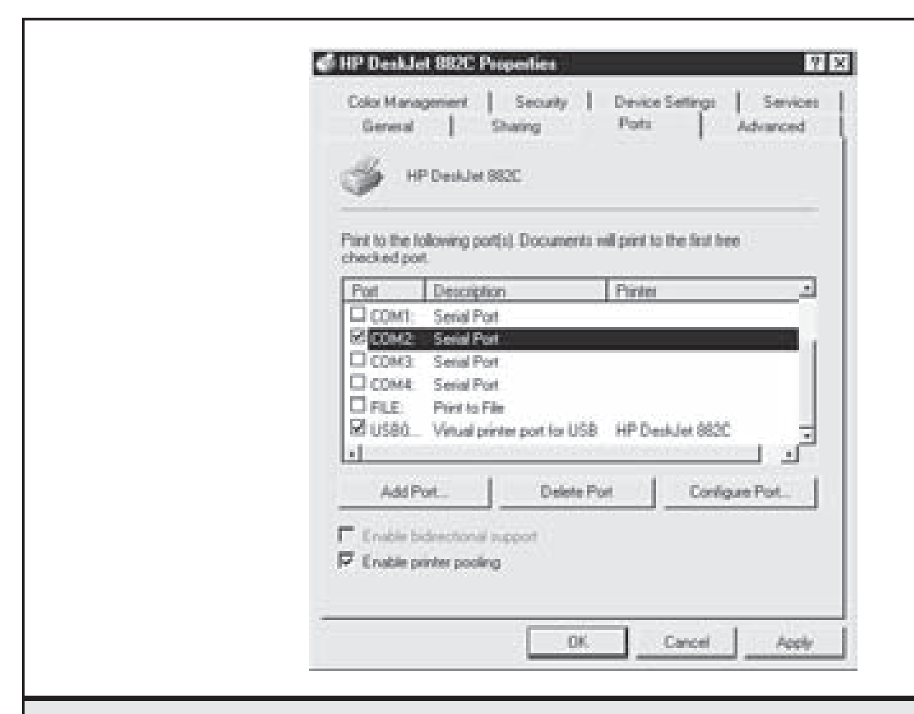


Figura 17-18. Permiso de poleo de impresoras.

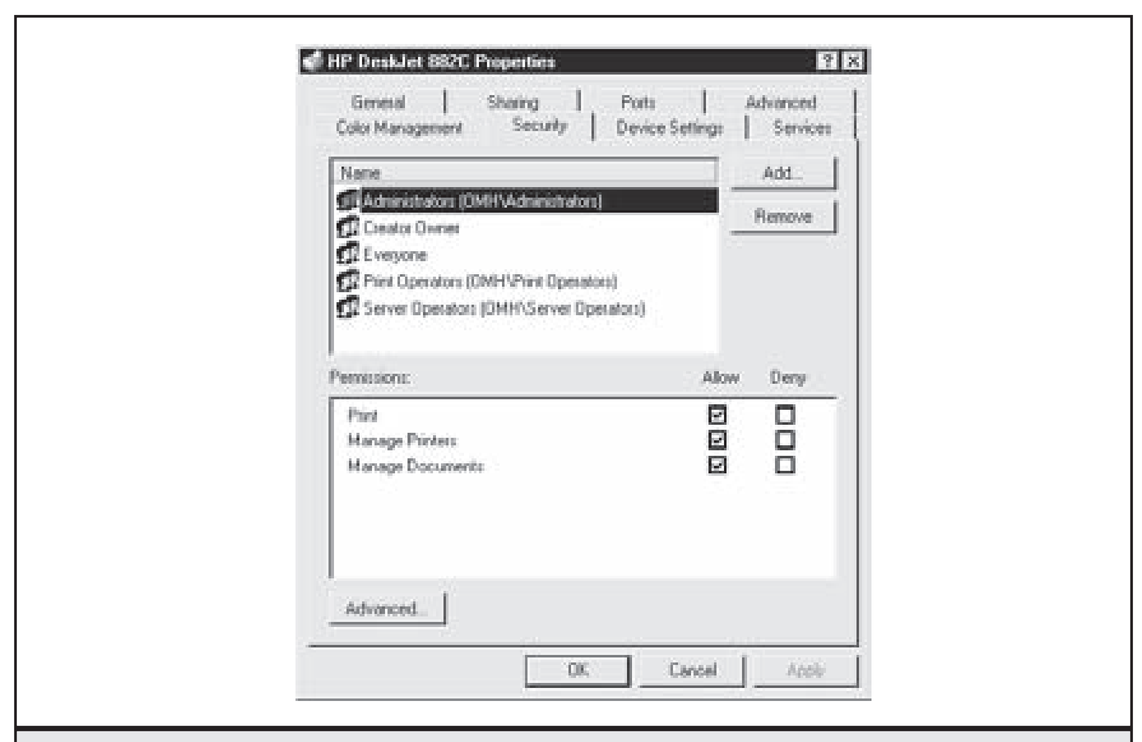


Figura 17-19. Configuración de los permisos de una impresora compartida.

puede observar, se asignan tres permisos principales a cada entidad: Print, Manage Printers y Manage Documents. El grupo Everyone tiene permiso para imprimir, pero no para administrar documentos que están en la cola. Sin embargo, un grupo especial llamado Creator Owner tiene permiso para administrar documentos. Esto significa que el usuario que envió el trabajo de impresión automáticamente tiene permiso para modificar o eliminar su propio trabajo de impresión, pero no así los demás trabajos que esperan en la cola.

▲ Windows 2000 Server puede almacenar los controladores de impresión adecuados para un gran número de diferentes clientes de Windows que se puedan conectar al servidor y utilizar sus impresoras. Por ejemplo, los controladores de impresión de una impresora en particular serán diferentes según la versión de Windows que corra la computadora del cliente, Windows 95, Windows 98, Windows NT 4, Windows 2000 o alguna otra. Cuando una computadora cliente abre una impresora compartida en la red, el controlador de impresión se instala automáticamente en la computadora cliente. Usted tiene control de este parámetro en la pestaña Sharing haciendo clic en el botón Additional Drivers, el cual muestra la caja de diálogo que aparece en la figura 17-20. Para agregar nuevos controladores, haga clic en los tipos de cliente adecuados que vayan a utilizar la impresora compartida en la red y,

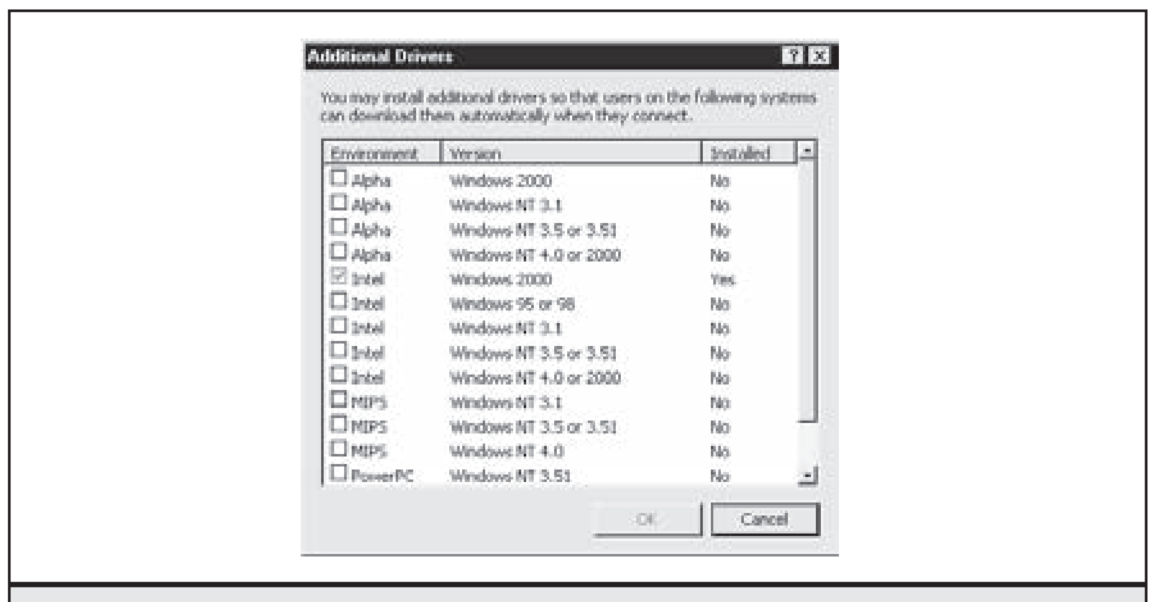


Figura 17-20. Carga de controladores de impresión adicionales para una impresora compartida.

después, haga clic en OK. El programa inmediatamente le pide los discos o CD-ROM correspondientes para instalar esos controladores. Después, Windows 2000 Server distribuye esos controladores de impresión entre las computadoras cliente cuando éstas utilicen por primera vez la impresora.

La configuración de las impresoras de red en Windows 2000 Server es un proceso relativamente directo que le brinda una flexibilidad considerable en cuanto a la forma en que usted configura y administra sus impresoras compartidas. Recuerde también que son posibles otros modelos de impresión como las impresoras conectadas a la red. Consulte la documentación que viene con dichas impresoras para encontrar los detalles acerca de cómo configurarlas en su red.

TRABAJO CON EL RESPALDO DE WINDOWS 2000

Para el administrador de la red, hay una tarea más importante que cualquier otra. Esta tarea no tiene nada que ver con asegurar la red contra los intrusos, dar mantenimiento a los usuarios, diseñar nuevos segmentos de red o resolver problemas en el servidor o las estaciones de trabajo. ¿Qué es entonces? Hacer respaldos de los datos regulares y confiables del sistema.

Tener la precaución de hacer respaldos regulares y confiables es, a menudo, un trabajo subvalorado, *¡hasta que sucede algo malo y son necesarios los respaldos*, en cuyo punto se convierte en el trabajo más reconocido de la compañía! Y no vaya a cometer un error al respecto: aunque las computadoras actuales son más confiables que nunca, existe todavía una gran variedad de formas en las que pueden fallar y perder o echar a perder información importante. Recuerde: solo existen dos tipos de administradores de red: los que han tenido fallas serias en el sistema y los que las tendrán. Sin embargo, las fallas de hardware no son los únicos criminales: las aplicaciones o los

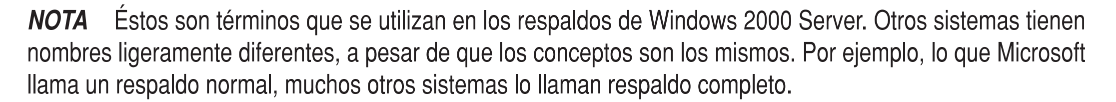
usuarios a menudo cometen errores que provocan la pérdida de información importante. Por tanto, contar con buenas copias de los datos en múltiples cintas puede eliminar este peligro.

Antes de profundizar en los detalles de cómo trabaja el software de respaldo de Windows 2000 Server, usted debe revisar algunos términos clave y conceptos importantes relativos a los respaldos.

Cada objeto, archivo y fólder de un servidor tiene un gran número de bits de atributos asociados con él. Algunos designan los archivos como de solo lectura, archivos del sistema o inclusive archivos escondidos. Uno se llama archivo (a menudo se conoce con el nombre de *bit archivo*), el cual marca si un archivo ha sido respaldado. Windows 2000 Server mantiene un registro de los archivos que han sido modificados. En cualquier momento que se modifique un archivo en el disco, el bit de archivo se pone en "encendido". (Por lo general, esos bits se conocen como *activados*, que significa que están encendidos y fijados a un valor 1, o como *desactivados*, que señala que están apagados y fijados a un valor 0). Cuando usted respalda el sistema, los archivos respaldados tienen el bit archivo nuevamente apagado. Ésta es la forma en que el sistema sabe qué archivos necesita respaldar y cuáles ya han sido respaldados.

El tratamiento del bit de archivo de maneras diferentes genera los siguientes tipos de respaldo:

- **Respaldos normales** Incluye todo lo que se ha seleccionado para respaldarse sin considerar si los bits de archivo están activos. Todos los bits de archivo son apagados tan pronto como cada archivo es respaldado.
- **Respaldos de copia** Respalda todo lo que se ha seleccionado, sin considerar si los bits de archivo están activos. Sin embargo, no modifican el estado de los bits de archivo, los cuales permanecen inalterados. Los respaldos de copia se utilizan para hacer un respaldo sin afectar una secuencia de respaldos normal, incremental y diferencial.
- **Respaldos incrementales** Respaldan solo los archivos que tienen sus bits de archivo activados, donde el respaldo está configurado para dejar a los bits de archivo intactos.
- **Respaldos diferenciales** También respaldan solo los archivos que tienen sus bits de archivo activos, pero el respaldo está configurado para dejar los bits de archivo intactos.
- **Respaldos diarios** Es un tipo especial de respaldo en Windows 2000 Server que es un respaldo diferencial, excepto que respalda solo los archivos que se modificaron en un día determinado.



NOTA Éstos son términos que se utilizan en los respaldos de Windows 2000 Server. Otros sistemas tienen nombres ligeramente diferentes, a pesar de que los conceptos son los mismos. Por ejemplo, lo que Microsoft llama un respaldo normal, muchos otros sistemas lo llaman respaldo completo.

Ahora que ya comprendió los diferentes tipos de respaldos disponibles, puede considerar el uso de diferentes esquemas de rotación de cintas, los cuales utilizan todos estos diferentes tipos de respaldos.

El esquema más sencillo de respaldo solo implica llevar a cabo respaldos normales todas las noches y rotar las cintas. En este modelo, existen muchas maneras eficientes de rotar las cintas. Una de las mejores que no consumen muchas cintas es etiquetar cuatro de ellas con los nombres "Lunes" a "Jueves" y utilizarlas en esos días. Después, etiquete cuatro cintas como "Viernes 1", "Viernes 2", hasta "Viernes 4", y rótelas cada semana. Después, haga una cinta al final del mes, el

último día del mismo, y consérvela para siempre. Este esquema es un buen balance entre utilizar cintas y poder ir hacia atrás en el tiempo para recuperar archivos. Este esquema utiliza 20 cintas al año, en cuyo punto usted probablemente las reemplace.

PISTA Sin importar qué tipo de esquema de rotación de cintas utilice, una buena idea es configurar una cinta llamada "Archivo de empleado". Siempre que un empleado abandone la compañía, grabe sus archivos en esa cinta antes de removerlos del sistema y mantenga una lista de los empleados que están en la cinta. Esto le proporcionará una referencia rápida y una fuente de recuperación disponible en caso de que los archivos de una persona en particular fueran necesarios en el futuro (lo cual pasa a menudo).

Otro esquema de rotación de cintas involucra el uso de las mismas cintas como se describió en el esquema anterior, pero también implica hacer respaldos completos (normales) del sistema todos los viernes por la noche y respaldos incrementales de lunes a jueves por las noches. Debido a que sólo los archivos modificados se respaldan durante la semana, se llevan a cabo rápidamente. La principal desventaja de este esquema es que si el sistema se cae el viernes por la mañana, usted debe recuperar muchas cintas a fin de poner al sistema en estado de respaldo más reciente. Primero, deberá recuperar el respaldo normal del viernes anterior y, después, recuperar cada una de las cintas incrementales, en secuencia, hasta el día en el que el sistema se cayó. El riesgo inherente de este esquema es el siguiente: ¿Qué haría si una de esas cintas se dañara? Su esquema completo de respaldo podría arruinarse si una de las cintas no funcionara correctamente. Aunque las cintas dañadas pueden representar un alto costo en cualquier esquema, dicho costo es muy alto especialmente en éste.

PISTA Aunque el programa de respaldos que está incluido en Windows 2000 Server no proporciona dicha facilidad, la mayoría de las soluciones de respaldo de una tercera instancia incluyen los esquemas de rotación automática de cintas. Dichos esquemas mantienen un registro de las cintas que usted necesita, cuánto tiempo las ha utilizado y cuáles necesita para recuperar cualquier conjunto de archivos. El uso del esquema de rotación incluido de cualquier software de respaldo de una tercera instancia es, en general, simple y trabajan bien.

Una forma de evitar las limitaciones del esquema anterior es el uso de respaldos diferenciales durante la semana, en lugar de usar respaldos incrementales. En consecuencia, usted debe hacer un respaldo normal todos los viernes por la noche y, después, un respaldo diferencial diario. Si tuviera que recuperar el sistema después de que se haya caído la mañana del viernes, todo lo que necesitaría recuperar serían dos cintas: una del viernes anterior y la del jueves por la noche. Esto se debe a que los respaldos diferenciales respaldan todos los archivos modificados desde el último respaldo normal. El respaldo diferencial de los lunes respalda los archivos modificados los lunes, el respaldo diferencial de los martes respalda los archivos modificados los lunes y los martes, etcétera.

NOTA Una buena idea es conservar un juego de cintas recientes fuera del sitio, en el caso de que un incendio o algún otro tipo de catástrofe destruya el cuarto de computadoras. Yo recomiendo enviar el respaldo completo anterior al más reciente de su sistema fuera del sitio y conservar la cinta más reciente para su uso. Este consejo se basa en que, con frecuencia, se presentan situaciones donde usted debe recuperar archivos rápidamente a partir del respaldo más reciente, por lo que debe tenerlos disponibles para este propósito. Sin embargo, usted también necesita conservar una cinta en rotación fuera del sitio que no pierda mucha información, en el caso de que suceda lo peor.

¿Existe algo que se llame muchos respaldos?

Si usted dio seguimiento al juicio del *Departamento de Justicia vs. Microsoft*, probablemente quedó perplejo ante toda la cantidad de correos electrónicos que el gobierno solicitó de la compañía. Estos correos electrónicos estaban disponibles ya que Microsoft contaba con buenos esquemas de respaldo de toda la información de su red y, aparentemente, la compañía nunca se deshizo de nada. Como el juicio lo demostró, ¡conservar todo no es necesariamente la mejor idea del mundo! Estoy seguro de que Microsoft respondería a la pregunta propuesta al comienzo de esta sección con una exclamación "¡Sí, debe contar con un gran número de respaldos!".

Comente con su departamento legal la posibilidad de establecer una política de retención de documentos y aplicarla a su base de datos de correo electrónico y respaldos. La mayoría de los departamentos legales están aterrorizados de verse involucrados en un pleito y que le soliciten "todos los correos electrónicos relacionados con tal o cual asunto de junio de 1993 a septiembre de 1999". Si usted se pusiera a pensar en el esfuerzo involucrado en satisfacer dicha solicitud, también se aterrorizaría. En el caso de un sistema de correo electrónico, la tarea significaría recuperar cada respaldo del periodo en cuestión y, después, buscar en la base de datos del correo electrónico, todos los mensajes que cumplan con el criterio, recuperar la cinta siguiente y repetir todo el proceso. Si usted cuenta con cientos de cintas de correo electrónico archivadas en el largo plazo, se verá en grandes problemas si trata de cumplir con dicha solicitud.

Aquí es donde lo pueden salvar las políticas de retención de documentos. Por ejemplo, usted puede trabajar con el departamento legal para establecer una política donde solo conserve cuatro cintas de respaldo de sus sistema de correo electrónico, dos cintas que rotan diariamente y dos que rotan cada semana. De forma que el lunes usted utiliza Daily A, el martes Daily B, y el miércoles usted sobrescribe Daily A con los datos del miércoles, etc. Usted hace lo mismo los viernes con las dos cintas semanales. Dicho esquema mínimo le da la oportunidad de recuperar el sistema de correo electrónico si algo llegara a suceder, pero no conserva cientos de copias al mismo tiempo. Por supuesto, cada compañía tendrá que hacer un balance entre la seguridad de tener más respaldos contra los riesgos que esto involucraría. Permítame repetirle: usted deberá trabajar con el departamento legal de su compañía antes de implantar este tipo de planes.

Utilización del software de respaldo de Windows 2000 Server

Windows 2000 Server incluye un programa de software de respaldo confiable y fácil de utilizar. A pesar de que no cuenta con todas las facilidades de algunos programas de respaldo disponibles de terceras instancias (como el ArcServe o el Backup Exec), funciona muy bien y satisface todas las necesidades. Para acceder al programa Backup, abra el menú Start y seleccione Programs, Accessories, System Tools y después Backup. Cuando usted comience a trabajar con el programa, lo primero que aparecerá será su pantalla de bienvenida, como se muestra en la figura 17-21.

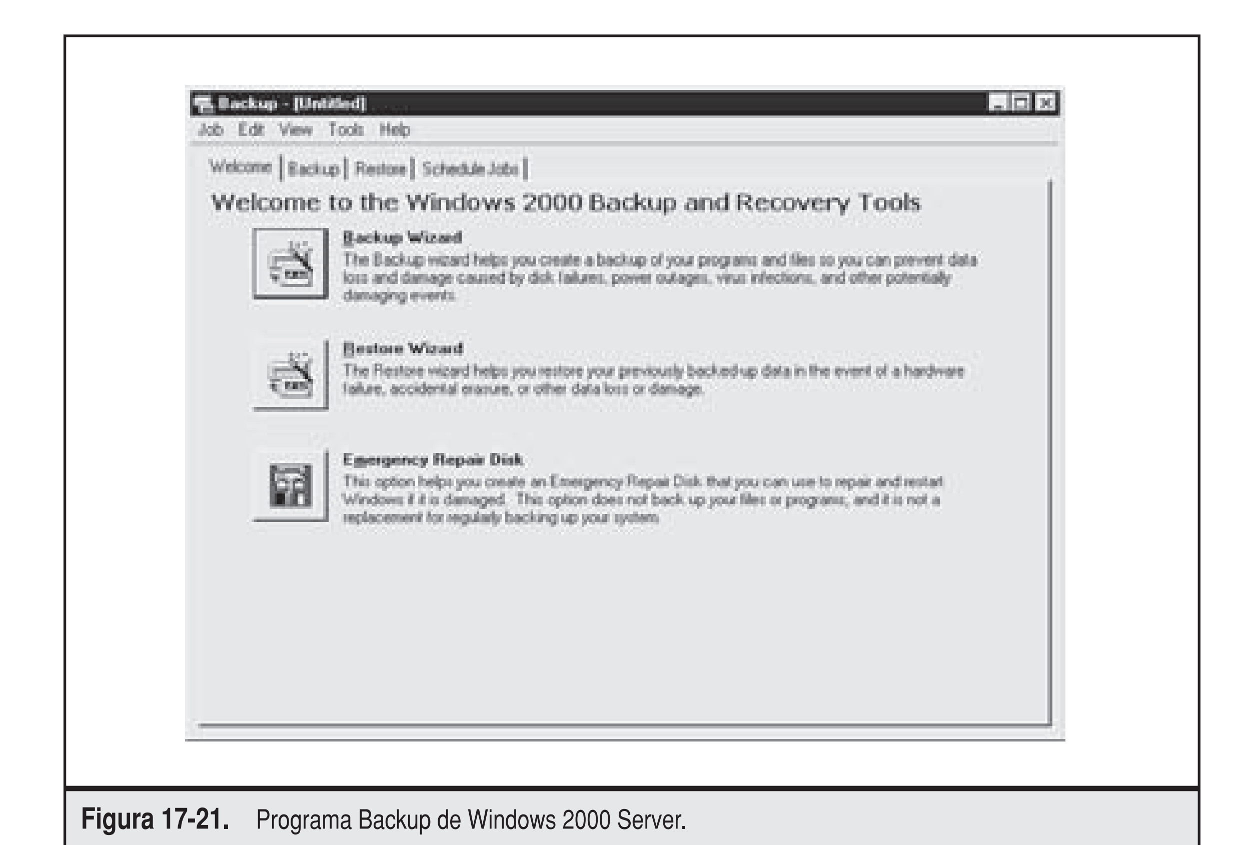


Figura 17-21. Programa Backup de Windows 2000 Server.

Backup lleva a cabo tres importantes tareas: respalda archivos, los recupera y le ayuda a preparase para la reconstrucción total del sistema en caso de una falla catastrófica. Los asistentes a los que se acceden por medio de la pestaña Welcome trabajan bien y le permiten utilizar cómodamente todas las facilidades del programa Backup.

Para configurar un respaldo, haga clic en el botón Backup Wizard sobre la pestaña Welcome y después clic sobre Next una vez que aparezca la pantalla de bienvenida del Backup Wizard. Enseguida, aparecerá la pantalla que se muestra en la figura 17-22.

Seleccione la opción adecuada, como Back up selected files, drives o network data, y después haga clic en Next para continuar. Enseguida, usted tendrá la oportunidad de seleccionar lo que desee respaldar con la pantalla Items to Back Up que se muestra en la figura 17-23.

Utilice las vistas del árbol del lado izquierdo para seleccionar los controladores, archivos u otra parte de la computadora que quiera respaldar. También puede seleccionar una categoría especial llamada *System State*, que incluye toda la información necesaria para reconstruir el Windows 2000 Server desde el principio, como los archivos clave del sistema, los datos del registro y cosas por el estilo. (Incluir el System State en la mayoría de los respaldos es una buena idea). Después de seleccionar lo que quiere respaldar, haga clic en Next para continuar. Usted podrá ver la caja de diálogo Where to Store the Backup que se muestra en la figura 17-24.

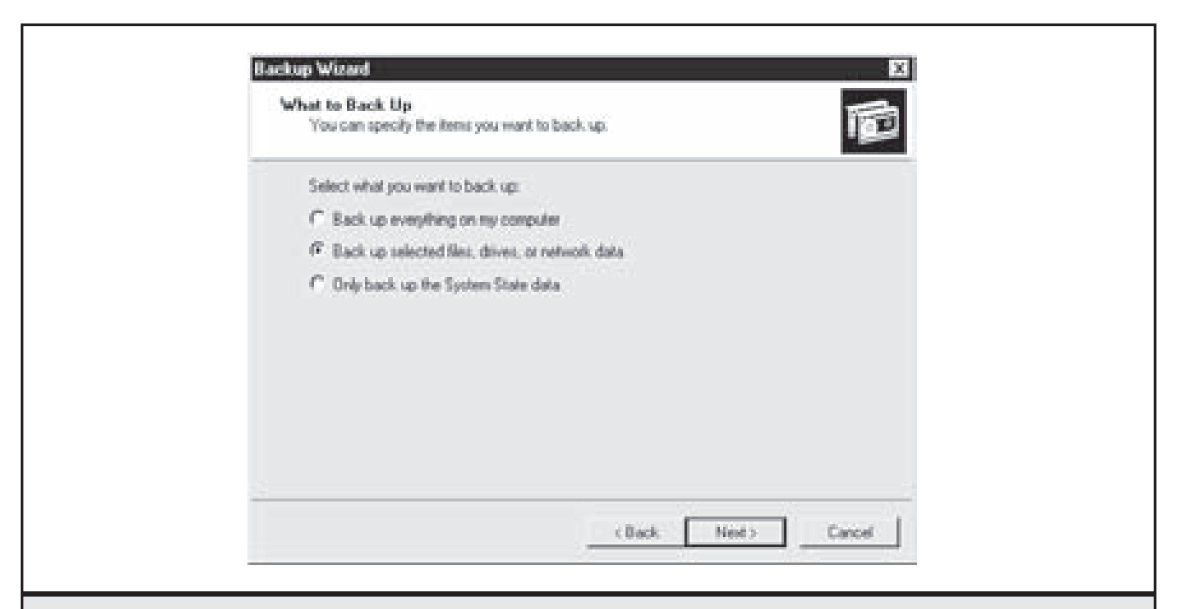


Figura 17-22. Selección de lo que desea respaldar con el Backup Wizard.

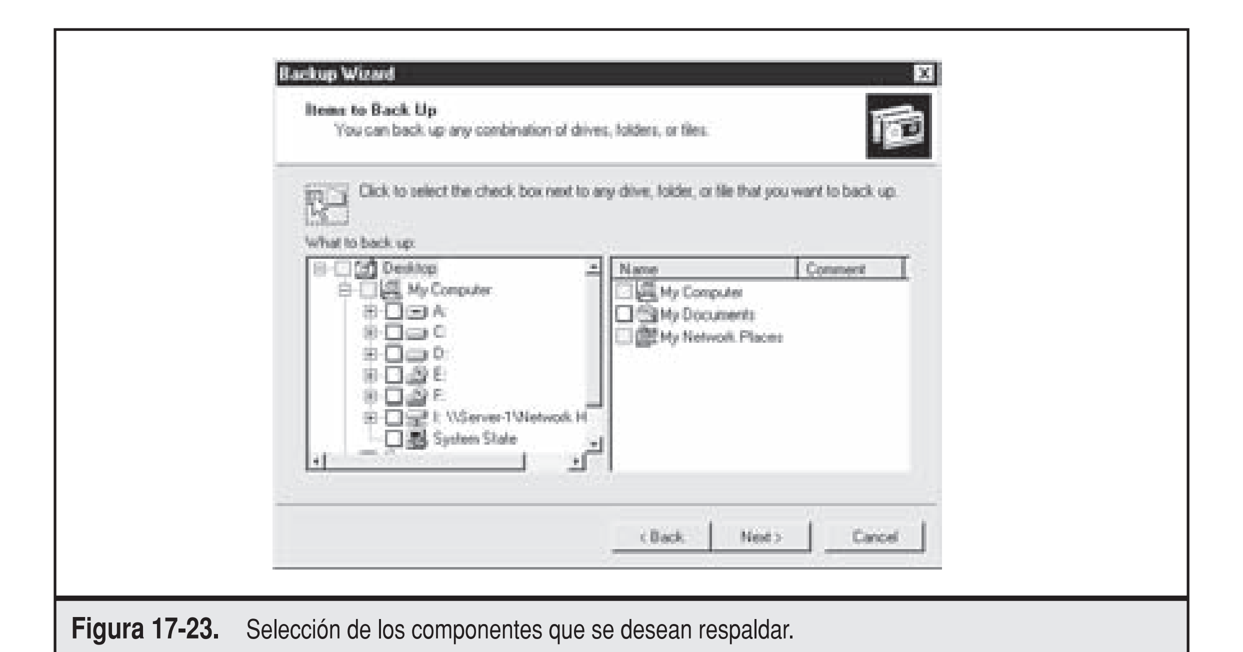


Figura 17-23. Selección de los componentes que se desean respaldar.



Figura 17-24. Selección de un destino de respaldo.

Una facilidad muy buena del programa Backup es que usted puede almacenar un respaldo en cualquier tipo de medio conectado a la computadora, incluyendo otro controlador de disco, algún medio removible como las cintas, CD escribibles (CD-R o CD-RW) o controladores JAZ o ZIP. En la caja de diálogo Where to Store the Backup, seleccione el tipo destino. Luego, si usted quiere realizar un respaldo basado en archivo, asigne un nombre al equipo de respaldo. Después de hacer clic sobre Next otra vez, verá una pantalla de confirmación que muestra todos los detalles pertinentes acerca del respaldo que desea preparar. En la pantalla de conformación se encuentra etiquetado un botón importante con el nombre de Advanced. Si hace clic en el botón Advanced se desplazará mediante otra secuencia de cajas de diálogo en las que podrá establecer las propiedades siguientes:

- Backup type, donde puede seleccionar los tipos de respaldo Normal, Copy, Incremental, Diferential y Daily.
- Verificar los datos de respaldo haciendo que el programa lo lea después de que sea escrito y comparando su contenido con el de la fuente para estar seguros de que el respaldo es correcto.
- Anexar o sobrescribir los datos de respaldo existentes sobre el medio que seleccionó.
- Una etiqueta para el equipo y medio de respaldo, si usted desea cambiar los nombres por omisión.
- Información acerca de la programación del respaldo, la cual puede utilizarse para programar que se lleve a cabo un respaldo más tarde, que también puede usarse para con-

figurar automáticamente trabajos de respaldo recurrentes, los cuales serán administrados por el servicio Scheduler de Windows 2000 Server.

Después de terminar los parámetros de Advanced, usted puede hacer clic en Next en la pantalla final Backup Wizard ya sea para comenzar el respaldo o para programar que comience a correr a la hora que lo haya programado.

Recuperar los archivos es más fácil que respaldarlos. Para ello debe utilizar la pestaña Restore o el Restore Wizard. Ambos métodos le piden primero que seleccione el medio o el archivo que utilizó para el respaldo desde el cual desea recuperar. Los métodos le permiten navegar a través de la lista de archivos respaldados y seleccionar los que desee recuperar. También tendrá la oportunidad de seleccionar ya sea sobrescribir los archivos o recuperar el respaldo en otro lugar del disco.

RESUMEN DEL CAPÍTULO

Ningún capítulo independiente podrá hacer justicia a todas las herramientas y el conocimiento necesarios para administrar al Windows 2000 Server de manera profesional. En este capítulo, sin embargo, usted pudo conocer cómo se manejan las tareas más comunes e importantes. Si administra o va a administrar un Windows 2000 Server, deberá tener un conocimiento aún más detallado acerca de los temas analizados en este capítulo y de las demás materias que necesitará dominar.

En particular, comience a investigar y a aprender acerca de estas importantes herramientas:

- Performance Monitor para reparar fallas, afinar el desempeño y supervisar en línea las estadísticas importantes del servidor. Performance Monitor puede configurarse para tomar ciertas acciones cuando se disparen las alarmas que usted programó, como el envío de una señal audible (beep) o de mensajes de alerta a otras computadoras de la red. Es también una herramienta extremadamente útil para resolver cualquier problema de desempeño que encuentre.
- La capacidad de Event Viewer para encontrar y diagnosticar problemas en Windows 2000 Server es clave. Usted debe utilizar Event Viewer de manera regular (yo recomiendo utilizarlo diariamente) para ver nuevos eventos y decidir si necesitan su atención inmediata. Usted puede utilizar Event Viewer para almacenar los reportes de Windows 2000 de forma periódica, creando un registro de largo plazo de mensajes de error e información almacenados en sus registros.
- Network Monitor es una herramienta avanzada para la captura de paquetes en la red y el despliegue de información acerca de ellos. También reporta las diferentes estadísticas de la red que puedan ser útiles para reparar problemas relativos al desempeño de la red.
- Scheduled Tasks puede utilizarse para programar tareas recurrentes que usted desee llevar a cabo frecuentemente en su servidor, como búsquedas de virus (con software de virus de otros proveedores), defragmentación de discos y prueba de éstos.

Éstas son algunas de las herramientas clave que usted debe aprender a utilizar para la administración básica de Windows 2000 Server. En el capítulo siguiente, también podrá leer acerca de otras herramientas utilizadas para administrar las facilidades avanzadas de Windows 2000 Server.



CAPÍTULO 18

Otros servicios de Windows 2000 Server

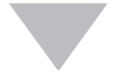
Una de las fortalezas de Windows 2000 es que puede hacer muchas cosas y cumplir con muchos roles. Windows 2000 Server no solo es un servidor de impresión y de archivos poderoso y eficaz, sino que también es extremadamente eficiente en el desempeño de muchas tareas una vez que se pone a funcionar.

Los capítulos anteriores le enseñaron cómo configurar Windows 2000 Server como un servidor de impresión y archivos básico y cómo administrarlo todos los días. Este capítulo presenta un panorama de otros servicios de Windows 2000 disponibles, pero hace hincapié en los servicios que proporciona este servidor. Para obtener el mayor provecho de él, usted necesita conocer qué servicios adicionales le puede prestar, cómo trabajan y qué hacen. Puede encontrar instrucciones detalladas acerca de cómo implantar estos servicios mediante un libro sobre Windows 2000 Server que estudie, a detalle, los servicios que desea instalar.

EXPLORACIÓN DEL PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE ANFITRIÓN (DHCP)

Si usted ha estado involucrado en las computadoras por mucho tiempo, probablemente recuerde cómo se administraban las direcciones TCP/IP manualmente (¡y quizá todavía lo siga haciendo!). Usted tenía que ir a cada computadora de la red para configurar su dirección TCP/IP de forma manual. También tenía que guardar un registro de qué computadoras usaban qué direcciones, ya que contaba con un número limitado con las cuales trabajar. Además, como probablemente sepa, cuando dos computadoras de la red tratan de utilizar la misma dirección TCP/IP, se presentan muchos problemas y se tiene que invertir tiempo en la solución de ellos.

DHCP le resuelve estos problemas. Un servidor DHCP es una computadora de la red que conserva un registro de las direcciones TCP/IP que están disponibles y las distribuye entre las computadoras y otros dispositivos que arrancan y solicitan una dirección IP del servidor. Con este tipo de servidor usted no necesita preocuparse acerca de los conflictos de direcciones ni de tener que reenumerar las que se utilizan en las computadoras si su rango de direcciones TCP/IP nunca se modifica (como usualmente sucede cuando usted cambia ISP en su conexión a Internet).



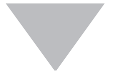
NOTA Debido a que TCP/IP es el protocolo por omisión de las redes basadas en Windows 2000 Server y a que este servidor está diseñado para funcionar correctamente solo en redes TCP/IP, los servicios DHCP son importantes y se encuentran instalados por omisión en Windows 2000 Server. Sin embargo, los servicios DHCP no están habilitados por omisión, puesto que es importante que nunca se configuren servidores DHCP en conflicto en una red.

Para utilizar el DHCP, usted debe definir un alcance y otros parámetros TCP/IP asociados, que los servidores asignan a las computadoras cliente. El *alcance* es simplemente el rango (o rangos) de direcciones TCP/IP que se le permite distribuir al servidor. Entre los parámetros asociados TCP/IP que el servidor distribuye se encuentran las direcciones de los servidores DNS o WINS que forman parte de la red. Cuando un servidor DHCP asigna una dirección TCP/IP a una computadora cliente, se dice que la dirección es *rentada* y se mantiene asignada a esa computadora cliente por un periodo fijo. En general, las rentas se configuran para que tengan una duración

de dos a siete días. (El parámetro por omisión de Windows 2000 es de ocho días). Durante este periodo, la dirección TCP/IP asignada no se le da a otra computadora.

Cuando una computadora cliente arranca y se une a la red, si está configurada para buscar un servidor DHCP, procede a buscarlo mientras inicia su pila de protocolos TCP/IP. Cualquier servidor DHCP que se encuentre disponible en ese momento responderá a la solicitud de una dirección por parte del cliente, con una dirección disponible en la base de datos del servidor DHCP. Luego, la computadora cliente utilizará esta dirección durante el periodo que dure su renta.

El administrador puede cancelar y reasignar información TCP/IP cuando sea necesario. (En general, lo hará después del horario de trabajo, cuando las computadoras cliente se encuentren apagadas). El administrador podrá entonces hacer modificaciones en la información referente al alcance del DHCP, la cual será comunicada posteriormente a los clientes cuando éstos se reconecten a la red. De esta forma, usted podrá fácilmente hacer cambios a información como direcciones DNS del servidor o más aún, rangos de direcciones TCP/IP, sin tener que ir a cada computadora.



PISTA Para acceder al DHCP en Windows 2000 Server, abra el menú Start, después seleccione Programs Administrative Tools | DHCP.

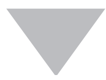
Aunque el DHCP es una magnífica herramienta para administrar direcciones TCP/IP, usted deberá utilizarlo en computadoras cliente que no almacenen ningún servicio TCP/IP que sea proporcionado a otras computadoras. Por ejemplo, no debe configurar un servidor web con DHCP para obtener una dirección TCP/IP dinámica ya que, entonces, las computadoras cliente que deseen conectarse al servidor web no podrán encontrar la dirección cuando ésta cambie. En lugar de eso, usted debe asignar direcciones fijas a computadoras que ofrezcan servicios que cuenten con TCP/IP ya sea a la red local o a través de Internet. Puede asignar estas direcciones en una de dos formas: primero, usted puede asignar localmente a esas computadoras direcciones TCP/IP fijas y después configurar *rangos de exclusión* al alcance que el servidor DHCP administre, lo cual evita que éste utilice u ofrezca esas direcciones a otras computadoras. Segundo, usted puede configurar una reservación en el servidor DHCP, la cual obliga al servidor a que siempre asigne la dirección reservada a una computadora específica.



PISTA Es una buena idea utilizar direcciones IP estáticas para sus impresoras de red, pues ello le permite que la reparación de problemas relacionados con la conectividad de la impresora sea más fácil.

INVESTIGACIÓN DEL SISTEMA DE NOMBRES DE DOMINIO (DNS)

DNS es una tecnología que permite recordar con facilidad los nombres que serán comparados con las direcciones y los puertos TCP/IP. Por ejemplo, cuando usted utilice un navegador de web e ingrese la dirección **http://www.yahoo.com**, utilizará un servidor DNS para encontrar el nombre de dominio **www.yahoo.com** que corresponde a una dirección TCP/IP en particular. Su navegador de la web utiliza transparentemente la dirección TCP/IP para comunicarse con el servidor en cuestión. El sistema DNS hace que Internet sea más fácil de usar. (Imagine qué emocionados estarían los anunciantes al decir "Visite nuestro sitio web en http://65.193.55.38!").



NOTA La información general del DNS se proporciona en el capítulo 8.

Windows 2000 Server incluye un servidor DNS completo. En realidad, se requiere un servidor DNS para que funcione el Directorio Activo. Si usted instala el primer servidor de Directorio Activo en un dominio Windows 2000, los servicios DNS se instalan de manera automática; de otra forma, tiene que seleccionarlos manualmente si desea agregarlos.

Usted administra los servicios DNS con el plug-in DNS Management Console, al cual usted accesa si abre el menú Start y selecciona Programs | Administrative Tools | DNS. La figura 18-1 muestra el plug-in del DNS.

Cuando instala el DNS en una organización, primero debe establecer un espacio de nombre raíz (un lugar virtual en el que se almacenan los nombres de dominio), generalmente utilizando el nombre de dominio que registró en Internet, como **ohm.com**. Luego puede crear sus propios subdominios apartando unidades organizacionales o geográficas, como **italy.ohm.com** o **accounting.ohm.com**. Un Windows 2000 Server que corra los servicios DNS puede administrar sus propios dominios y subdominios y usted puede también configurar múltiples servidores DNS, cada uno de los cuales administrará una porción del espacio nombre dominio. Cada servidor DNS es responsable del almacenamiento de todos los nombres DNS que se utilizaron para su espacio nombre administrado y para comunicar cualquier cambio a otros servidores DNS. Cuando usted utiliza servidores DNS múltiples para administrar porciones separadas de su espacio nombre DNS, cada servidor DNS administra una zona. Las actualizaciones entre

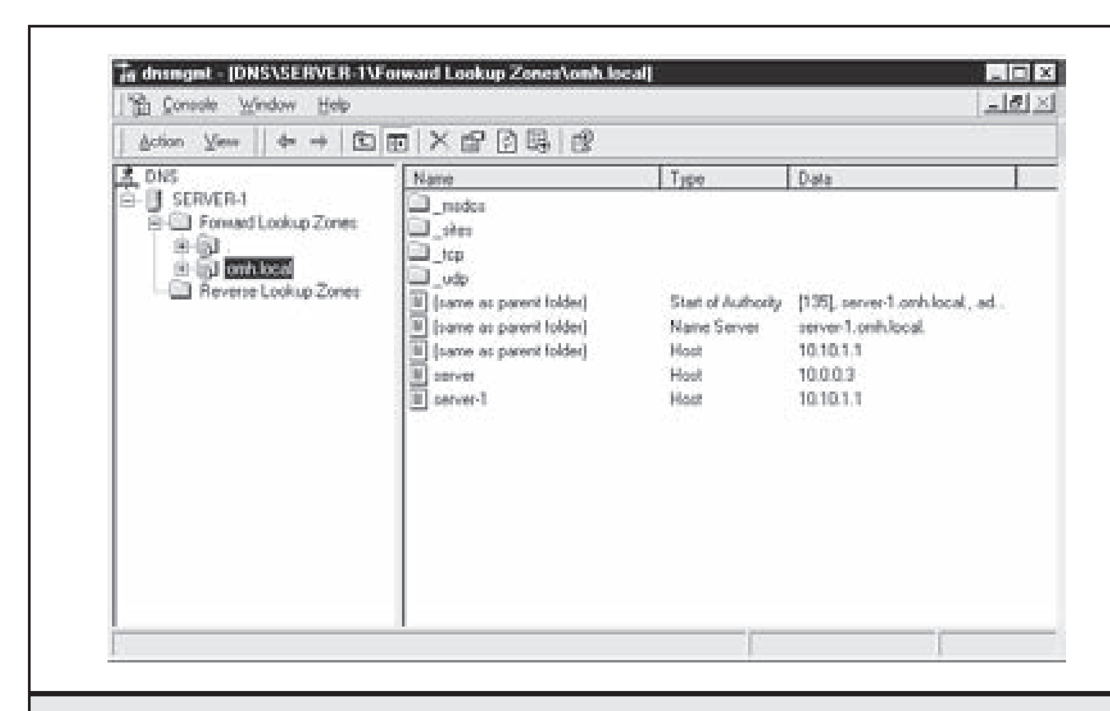


Figura 18-1. El plug-in de la DNS Microsoft Management Console (MMC).

diferentes zonas se llaman *transferencias de zona*. Los servicios DNS de Windows 2000 soportan tanto transferencias de zona completas como incrementales. (Las transferencias incrementales de zona intercambian solo información actualizada, que aligeran considerablemente el tráfico en las redes con muchos espacios nombre del DNS).

Debido a que el DNS es una parte integral del Active Directory, es importante que usted establezca redundancia para sus servidores DNS. Microsoft recomienda que cada controlador de dominio también actúe como servidor DNS, y deberá tener al menos un servidor principal y otro secundario para cada una zona administrada. (En redes pequeñas, es posible —y probablemente deseable debido a los problemas de costos— utilizar solo un servidor DNS).



NOTA Antes de Windows 2000 Server, las redes TCP/IP basadas en Windows utilizaban en realidad dos sistemas diferentes de nombres. El primero empleado con TCP/IP era DNS. El segundo, utilizado con NetBIOS y NetBEUI, era Windows Internet Name Service (WINS). En Windows 2000 Server, los servicios DNS pueden también configurarse para ofrecer servicios WINS a la red para las computadoras convencionales. Sin embargo, para navegar por la red la mejor alternativa posible es migrar al DNS.

COMPARACIÓN DEL SERVICIO DE ACCESO REMOTO (RAS) Y EL RRAS

El RAS (se pronuncia *razz*) ofrece una manera para que usted configure el soporte de marcación interna a su red donde las computadoras de cliente remoto forman una conexión de nodo remoto hacia la red mediante algunas formas de conexión conmutada. Estas conexiones pueden hacerse con módems y líneas telefónicas o con conexiones ISDN. (Por supuesto, ambos lados de la conexión RAS deben soportar el tipo de conexión que se utilice). Los servicios RAS le permiten configurar Windows 2000 Server fácilmente para que actúen como un servidor RAS en la red y los usuarios remotos puedan conectarse al servidor para poder acceder a los recursos de la red.

Routing and Remote Access Service (RRAS, que se pronuncia ar-razz) es también una tecnología de acceso remoto, pero incluye facilidades de enrutamiento que le permiten a las conexiones a la red a través de una red pública —como Internet— utilizar tecnología de *red privada virtual (VPN)*. Una VPN funciona mediante la instalación de un "túnel" seguro entre un cliente y el servidor RRAS a través del cual se transfieren los paquetes encriptados. La computadora cliente marca a su ISP normal de Internet y, después establece una conexión VPN segura con el RRAS a través de Internet.



NOTA La tecnología VPN se estudia en el capítulo 10.

RAS y RRAS se administran por medio de la misma herramienta en Windows 2000 Server. Abra el menú Start y después seleccione Programs | Administrative Tools | Routing and Remote Access para acceder al plug-in MMC. Después de que el plug-in se inicie, haga clic con el botón derecho del mouse en el servidor en el que desea permitir el acceso remoto y, posteriormente, seleccione Configure and Enable Routing and Remote Access. Un asistente muy útil lo guiará en el proceso y le permitirá seleccionar si habilita solo el acceso remoto, solo enrutamiento/acceso remoto, o ambos. La figura 18-2 muestra el plug-in Routing and Remote Access una vez que el RRAS ha sido habilitado.

Los servicios de acceso remoto bajo Windows 2000 Server son seguros y brindan una flexibilidad considerable para que usted pueda configurarlos en la forma que quiera. Primero, deberá habilitar a un usuario para acceder a la red de forma remota, lo cual puede hacer mediante la edición de la caja de diálogo Properties del usuario (vea el capítulo 17). Después, puede configurar el RRAS para que utilice un gran número de facilidades de control que le permitan mantener el acceso remoto en forma segura, lo cual incluye:

- Establecer horas y días cuando se desee que el acceso remoto funcione.
- Establecer horas y días en los cuales usuarios y grupos específicos puedan utilizar el acceso remoto.
- Limitar el acceso solo al servidor RRAS o a los servicios específicos de la red.
- Utilizarlas facilidades de retro-llamada, que permiten que un cliente remoto marque hacia la red e ingrese a ella. Después, la red desconecta la conexión y marca al usuario a un número telefónico predefinido.
- Establecer políticas de acceso con base en el nombre de la computadora del cliente remoto o la dirección TCP/IP.

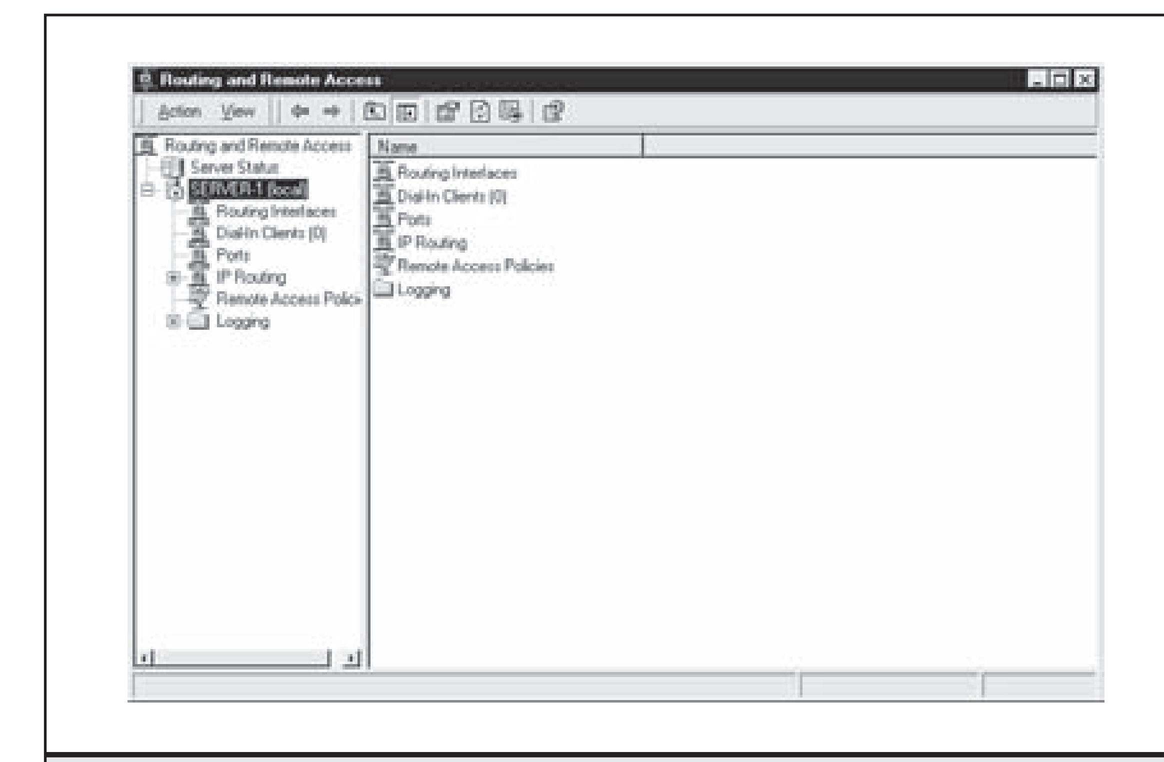


Figura 18-2. Utilice el plug-in Routing and Remote Access MMC para administrar el acceso remoto.

Por medio del uso del RAS y el RRAS, usted puede fácilmente configurar el Windows 2000 Server para ofrecer a los usuarios remotos importantes servicios de acceso seguro, tanto a través de conexiones telefónicas como de Internet.

EXPLORACIÓN DEL SERVIDOR DE INFORMACIÓN DE INTERNET (IIS)

Windows 2000 Server incluye una serie de servicios de Internet que se ofrecen como parte de IIS. El IIS incluye servicios FTP, SMTP y NNTP, cada uno de los cuales puede iniciarse o detenerse de manera independiente. El IIS se administra mediante un programa Internet Services Manager que se encuentra en el grupo de programas Administrative Tools. La figura 18-3 muestra el Internet Services Manager.

Los servicios de web IIS ofrecen un software anfitrión de web muy completo. Usted puede definir múltiples sitios web con el IIS, cada uno de los cuales es administrado de manera independiente. Para cada sitio, usted especifica el directorio en el que pueden encontrarse los archivos de cada uno así como los parámetros de seguridad para ese sitio y los parámetros de desempeño para optimizar su desempeño.

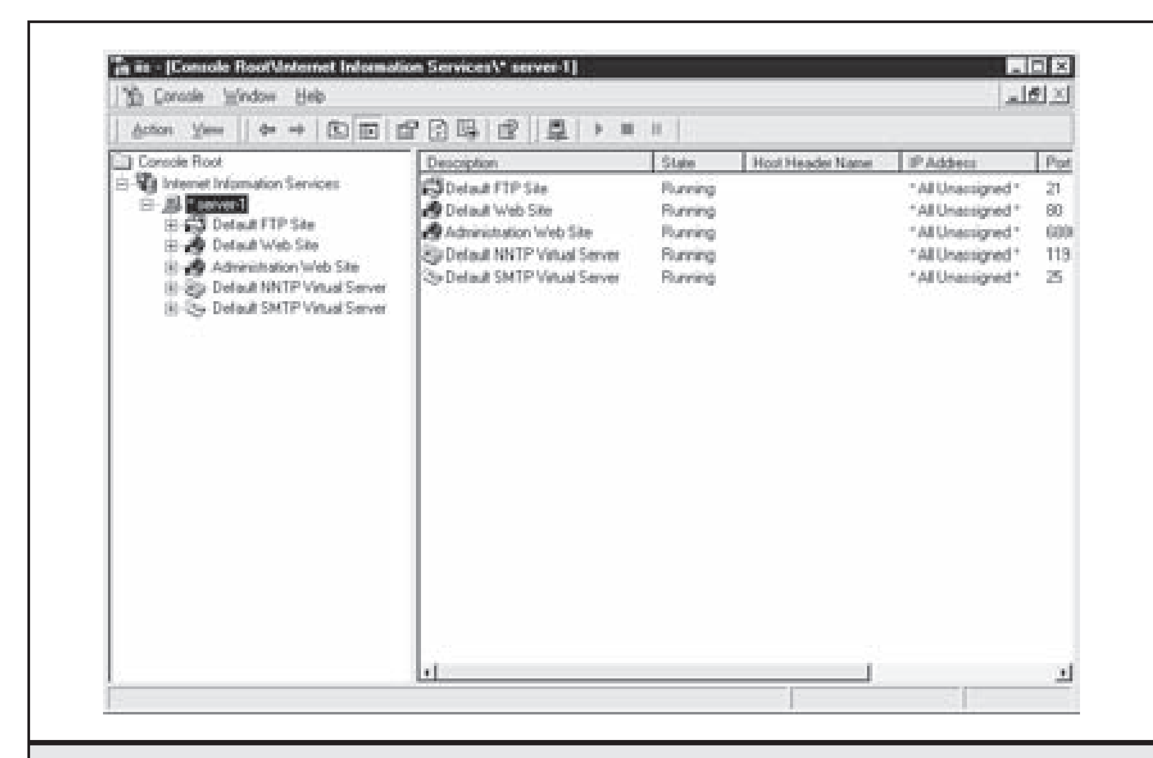


Figura 18-3. Internet Information Services Manager proporciona un solo lugar desde el cual administrar los servicios de Internet.

Los servicios FTP del IIS le permiten configurar un sitio FTP en una computadora con Windows 2000 Server. Usted define el directorio FTP, así como si las listas de directorio se mostrarán en formatos estilo UNIX o MS-DOS. También puede fijar los parámetros de seguridad para permitir, o no, que las diferentes computadoras cliente o redes cliente accedan al servidor FTP y especificar si va a permitir accesos FTP anónimos.

El servidor NNTP en el IIS le permite configurar su propio sitio estilo Usenet mediante el empleo del protocolo NNTP. Los clientes pueden conectarse a su servidor NNTP a través de herramientas, como Outlook Express u otros lectores de noticias Usenet.

Por último, el servidor *Simple Mail Transfer Protocol (SMTP)* permite que se puedan formar conexiones SMTP entre el sistema que corre bajo IIS y los sistemas de correo remoto SMTP. El SMTP es el protocolo estándar para intercambiar correo electrónico a través de Internet.

EMPLEO DE SERVICIOS DE GRUPO

Windows Cluster Services le permite combinar dos o más servidores en un cluster. Puede configurar estos agrupamientos para cumplir con uno de los dos papeles que juegan los agrupamientos:

- Los agrupamientos para el balanceo de la carga de la red le permiten compartir servicios basados en TCP/IP —como el servidor de web— entre hasta 32 servidores Windows 2000.
- Los *agrupamientos de servidores* proporcionan soporte contra fallas en caso de que uno de los servidores falle. Los dos servidores comparten un arreglo de disco común así como el acceso al arreglo de los diferentes servicios y aplicaciones que cada uno corre. Usted puede llevar a cabo el balanceo de carga limitado si corre algunos servicios en un servidor y otros en otro. Si uno de los servidores falla, el otro retoma sus tareas de forma transparente. Los agrupamientos de servidores también le permiten transferir servicios de un servidor a otro, lo cual es de mucha utilidad cuando se realizan actualizaciones de agrupaciones que funcionan sin tener que sacar de operación al agrupamiento.

Los Cluster Services son una herramienta invaluable para construir redes de alto desempeño y disponibilidad. Sin embargo, la instalación, el cuidado y la alimentación de los agrupamientos son temas complicados. Si necesita utilizar agrupamientos, debe leer cuidadosamente la documentación de Microsoft relativa a su instalación y mantenimiento, y considerar la compra de un libro que se dedique al estudio de los agrupamientos en Windows 2000.

SERVICIOS DE TERMINAL DE WINDOWS

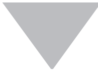
El último servicio que se estudia en este capítulo, pero que posiblemente es uno de los más útiles, es el *Windows Terminal Services (WTS)*. Los WTS le permiten instalar un Windows 2000 Server casi como si fuera un equipo grande, esto es, donde las terminales puedan conectarse y todo el trabajo lo llevará a cabo una computadora central, la cual, en este caso, sería una computadora Windows 2000 Server. Una computadora cliente se conecta al Servidor Terminal mediante una conexión TCP/IP, ya sea a través de una conexión conmutada o una conexión LAN/WAN y se firma en el sistema. De ahora en adelante, la computadora cliente es responsable solo de desplegar pantallas

y aceptar la entrada del teclado y del ratón; todo el trabajo, en realidad, lo lleva a cabo el Terminal Server por medio de la creación de una máquina virtual Windows en el servidor. Un *Terminal Server* puede crear muchas máquinas virtuales Windows, cada una de las cuales realiza sus propias tareas y corre sus propios programas.

¿Cuándo utilizará una conexión Terminal Server en una red en lugar de una conexión de nodo remoto, como las proporcionadas vía RAS y RRAS? La respuesta depende de un gran número de factores, de los cuales pueden ser considerados los siguientes:

- La computadora remota no cuenta con los recursos adecuados para correr algunas aplicaciones y llevar a cabo alguna tarea. Si corre sus programas en la Terminal Server, la computadora remota puede aprovechar los recursos de éste. Por ejemplo, suponga que una aplicación en particular corre en forma óptima solo cuando cuenta para trabajar con 2 GB de RAM. En un caso como éste, un simple cliente Windows XP con 384 MB de RAM puede conectarse al Terminal Server (que tiene 2-4 GB de RAM) y corre la aplicación en cuestión. De manera similar, algunas aplicaciones pueden requerir muchos procesadores o acceso directo a arreglos grandes de discos o a algún otro recurso local al que el Terminal Server tenga acceso.
- A través de conexiones de poco ancho de banda, por módem a 33.6 Kbps, algunas aplicaciones trabajan de manera más eficiente utilizando una forma de control remoto que el método del nodo remoto. La mayoría de las conexiones de acceso remoto son de bajo ancho de banda y, sin embargo, algunas aplicaciones necesitan gran ancho de banda para trabajar adecuadamente. Debido a que la computadora remota conectada al Terminal Server solo tiene que transferir información de despliegue y de entrada, la aplicación que corre en el Terminal Server puede hacerlo de una manera más rápida que la que lo haría a través de una conexión de nodo remoto.
- Algunas aplicaciones y tareas, como la administración de un Windows 2000 Server, no pueden llevarse a cabo totalmente por otra computadora incluso si ésta contara con una conexión que corriera a velocidades de LAN. Los Terminal Services permiten que una computadora remota corra esas aplicaciones solo si cuenta con los permisos apropiados. Por ejemplo, suponga que su compañía tiene una red remota localizada en algún lugar de Asia, pero que la red no fuera lo suficientemente grande como para justificar un administrador local. Si utiliza los Terminal Services, usted podría conectarse a esa red a través de la WAN de la compañía y llevar a cabo todas las tareas administrativas, como la configuración de los discos duros, las comparticiones (recursos compartidos), los protocolos de red adicionales, etcétera.

Ciertas aplicaciones podrían requerir el uso de los Terminal Services. Sin embargo, en cualquier caso, usted deberá considerarlos como un plus a los servicios de acceso remoto. Si tuviera que proporcionar soporte a muchos usuarios remotos, encontrará que algunos de ellos tienen necesidades que se satisfarían mejor con conexiones a nodos remotos y otros tendrían necesidades que se cubrirían mejor con conexiones de control remoto. Correr ambos servicios en su red le proporcionará una flexibilidad adicional considerable en el soporte de los usuarios remotos y en la resolución de cualquier problema que ellos pudieran encontrar.



NOTA Si usted implanta Terminal Services, asegúrese de revisar cuidadosamente el acuerdo de licencia de Microsoft y los modelos de cobro, los cuales difieren cuando utiliza los Terminal Services.

RESUMEN DEL CAPÍTULO

La familia de Windows Server, que incluye el Windows 2000 Server, es quizás el ambiente NOS más rico disponible en la actualidad. Mientras que otros productos NOS pueden llevar a cabo todos las tareas que se describen en este capítulo, ninguno incluye todas las facilidades que ofrece NOS, sino que requieren compras adicionales. Debido a la gran cantidad de facilidades que proporciona el Windows 2000 Server, usted podrá conformar más fácilmente un servidor que satisfaga casi cualquier necesidad que pueda tener. Y debido a que los diferentes servicios Windows 2000 Server trabajan muy bien en conjunto, ¡usted podrá implantar fácilmente casi todos estos servicios avanzados en un solo servidor! Esta flexibilidad "fuera de la caja" y facilidad de administración es una de las razones que explica por qué la familia Windows Server de sistemas operativos de red ha ganado una ventaja competitiva en el mercado de los NOS, por qué ha logrado un lugar en el mercado tan rápidamente en los últimos años y por qué es muy probable que Windows 2000 Server continúe con esta tendencia.

CAPÍTULO 19

Windows Server 2003

Este capítulo estudia el programa Windows Server 2003 de Microsoft, uno de los adelantos más grandes en la línea de servidores Windows Server en años.

A medida que las redes migran de Windows NT 4 y Windows 2000 Server a Windows Server 2003, los profesionales de la conectividad de redes necesitan comprender las mejoras en éste.

LAS NUEVAS CARACTERÍSTICAS DE WINDOWS SERVER 2003 DE MICROSOFT

Windows Server 2003 es una actualización importante de la familia de productos Windows 2000 Server, con mejoras de gran alcance en cuanto a seguridad, desempeño y características específicas del lado del servidor. El objetivo de Microsoft, en el Windows Server 2003, fue hacer un sistema operativo de servidor tan bueno como cualquiera de los sistemas operativos UNIX, lo cual se cumplió. Mientras que las familias de los servidores Windows se han comparado siempre de manera favorable con UNIX en cuanto a su facilidad de uso y administración, éste ha sido siempre mucho más confiable y, en general, se desempeña mejor con un hardware equivalente. Por ejemplo, la mayoría de los servidores UNIX funcionan por años sin que su desempeño demerite o sin que se presenten errores. Por otro lado, los servidores Windows necesitan ser reiniciados profilácticamente a intervalos regulares de tiempo (cada mes, por decir algo), a fin de evitar los errores acumulados que se pudieran presentar a partir de fugas de memoria y otros tipos de problemas.

Ediciones de Windows Server 2003

Windows Server 2003 se ofrece en cuatro ediciones diferentes; cada una tiene un precio y un conjunto de características específicos. Estas ediciones son:

- **Standard Server** es la versión más básica de Windows Server 2003. Tiene todas las características de la familia Windows Server 2003, excepto por las siguientes particularidades: servicio cluster, soporte a servicios de metadirectorio, soporte de procesadores Itanium, capacidad de agregar memoria con el equipo en funcionamiento, acceso no uniforme de memoria y varias características específicas del Datacenter Server. El Standar Server no soporta una arquitectura de 64 bits, soporta un máximo de 4 GB de RAM instalada y puede utilizar hasta cuatro procesadores.

- **Enterprise Server** es el término medio de los ofrecimientos de Windows Server 2003. Incluye todas las características de la familia Windows Server 2003, excepto las características específicas del Datacenter Server. El Enterprise Server es análogo al Windows 2000 Advanced Server. El Enterprise Server está disponible en una versión de 64 bits y puede soportar hasta 32 GB de RAM (64GB en la versión de 64 bits) y hasta ocho procesadores.

- **Datacenter Server** es la versión de mayor desempeño de Windows Server 2003, está orientada a cargas de tráfico extremadamente elevadas sobre el hardware de servidor más capaz. Incluye todas las características de la familia de Windows Server 2003, pero no puede compartir la conexión a Internet ni la firewall. El Datacenter Server soporta una arquitectura de 64 bits, puede hacer uso de hasta 64 procesadores y puede manejar hasta 64 GB de RAM (hasta 512 GB en la versión de 64 bits).
- **Web Server** está diseñado para realizar tareas de servidor de web. Esta versión es apropiada sólo para actuar como un servidor web, ya que adolece de muchas características del resto de la familia Windows Server 2003. Sin embargo, esto no es malo, pues si diseña un servidor web utilizando Windows Server 2003, muchas de las particularidades principales del servidor son superfluas, y quitarlas reduce el precio del Web Server incluso a un costo mucho menor que el Standard Server. Además, no tiene por qué preocuparse por la administración de características extrañas ni de cualquier otra interferencia que pudieran provocar con la tarea de trabajar como un servidor web. El Web Server no se encuentra disponible en la arquitectura de 64 bits y puede soportar hasta dos procesadores y 2 GB de RAM instalada.

Características nuevas y mejoradas en Windows Server 2003

Microsoft ha incorporado una plétora de nuevas características a la familia Windows Server 2003 relacionada con la familia Windows 2000 Server. Esta sección ofrece una introducción a las mejoras y adiciones principales de Windows Server 2003 en comparación con Windows 2000 Server.

Directorio Activo

El Directorio Activo (active directory, AD) ha sido mejorado en una gran variedad de formas, dentro de las que se incluyen:

- Replicación del AD en 5 000 servidores. (Windows 2000 soportaba solo hasta 200 servidores AD para replicación).
- Un desempeño más rápido por medio de mejorar cómo funciona el Global Catalog, incluyendo contraseñas de usuario almacenadas en el caché para usuarios remotos y una replicación más eficiente entre los servidores de Global Catalog.
- Nuevas cualidades administrativas: ahora se pueden administrar múltiples objetos AD de manera colectiva, las herramientas de la Consola de Administración de Microsoft del AD soportan ahora la facilidad de arrastrar y pegar, así como otras mejoras, y los dominios ahora pueden ser renombrados.
- Existe ahora una nueva característica llamada Forest Trust, donde los forests AD pueden confiarse entre sí y la información sobre seguridad de los usuarios puede compartirse entre los forests.

Servicios Cluster y de aplicación

Windows Server 2003 contiene una gran cantidad de mejoras en cuanto a su soporte a aplicaciones enfocadas a él, siendo las más notables las relacionadas con la inclusión de la estructura .NET de Microsoft.

Los servicios de agrupamiento (disponibles solo en las ediciones Enterprise Server y Datacenter Server) han sido mejorados para proporcionar soporte hasta a ocho agrupamientos de nodos. Windows 2000 soportaba únicamente dos nodos (2000 Advanced Server), o bien, cuatro nodos (2000 Datacenter Server). Ha habido una gran cantidad de avances en el agrupamiento que ha dado como resultados una administración más fácil y un mejor balanceo en la carga de la red.

Servicios de impresión y de red

Es probable que existan más servidores de Windows en uso abocados a servicios de archivo e impresión que de cualquier otra tarea para la que instala un servidor. Debido a la importancia de los servicios de archivo e impresión, las mejoras en esta área de Windows Server 2003 deben ser del interés de casi cualquier organización. Estas mejoras incluyen:

- Recuperación automática del sistema, en la que puede recuperar un sistema operativo, su estado y su configuración de hardware en un solo paso. Lo anterior hace que la recuperación del servidor (debida, por ejemplo, a una falla en el disco duro) sea más fácil y rápida que antes.
- Avances en la defragmentación del disco: Disk Defragmenter corre mucho más rápido que en Windows 2000, puede defragmentar la Master File Table (MFT) en línea, y ahora puede ser llamada desde un script (de manera que pueda programar la defragmentación para que ocurra cuando la demanda en el servidor sea baja).
- El programa CHKDSK corre dos veces más rápido en Windows Server 2003 que en Windows 2000 Server.
- Contiene muchas herramientas de línea de comando nuevas para la administración de servicios de archivos e impresión: muchas tareas administrativas son difíciles de automatizar por medio de una interfase gráfica de usuario, en particular para los administradores con experiencia. Las nuevas herramientas de línea de comandos en Windows Server 2003 pueden quizá parecer un retroceso, pero en realidad ofrecen alternativas más poderosas para la administración de sistemas.
- Volume Shadow Copies es una nueva facilidad en Windows Server 2003. Cuando se habilita, el sistema verifica los archivos en el momento que usted especifique. Si los archivos son modificados o borrados de su sistema, aún existen versiones más antiguas en el área de copia de sombra o de respaldo (shadow copy area) del disco. (Usted define cuánto espacio en disco quiere ocupar en esta facilidad; Microsoft recomienda 10 por ciento). Las copias de sombra almacenan únicamente las diferencias, por lo que son muy eficientes. (Por ejemplo, cada punto de verificación no almacena una copia completa del contenido del disco, sino solo los cambios). Los usuarios pueden entrar de manera fácil a esta característica para recuperar versiones más antiguas o eliminadas de su trabajo, en lugar de tener que solicitar al departamento de IT que las recupere de la cinta. En algunas organizaciones esto puede ahorrar mucho tiempo al usuario y al administrador de red y hacer recuperables los archivos que no se hayan podido salvar, aun desde la cinta.
- El programa de respaldo incluido en Windows Server 2003 puede respaldar archivos abiertos, utilizando la cualidad de copia de sombra para respaldar archivos que se encuentren abiertos.

Servicios de Internet

Los servicios de Internet han cobrado importancia en todos los servidores, y no solo en aquellos que ofrecen servicios web o de otro tipo.

Los Servicios de Información de Internet 6.0 (IIS, del inglés Internet Information Services) están incluidos en todas las versiones de Windows Server 2003. Su desempeño ha sido mejorado de forma radical mediante un nuevo programa llamado HTTP.SYS, el cual corre ahora en modo kernel. (Recuerde que en los sistemas operativos Windows NT/2000/XP, los componentes corren ya sea en el modo Usuario —en el que el sistema por sí mismo se protege de errores en el componente a expensas del desempeño—, o en el modo kernel —en el que un componente tiene control total del sistema, con muy poca o ninguna protección en otros procesos que se encuentren corriendo—. Los componentes del modo kernel corren mucho más rápido que los componentes del modo usuario). El programa HTTP.SYS es responsable de responder a las solicitudes de protocolo HTTP hechas por el IIS y se utiliza de manera extensiva para llevar a cabo tareas de servidor web.

En respuesta al gran número de problemas de seguridad de IIS en las versiones anteriores de los servidores Windows, el IIS 6.0 ahora omite un estado de "candado" cuando se instala. Lo anterior evita que un administrador, sin darse cuenta, deje un servidor más expuesto a un ataque de lo que sea estrictamente necesario para los servicios que se necesiten.

IIS 6.0 también tiene una arquitectura mejorada, por medio de una variedad de medidas. Primero, los recursos (como la memoria del sistema) están distribuidos de manera dinámica, lo que permite que un número mucho más grande de sitios web sean almacenados en un solo servidor. Segundo, nuevas cualidades hacen que el IIS sea más confiable, como la habilidad del IIS de supervisar la salud de sus procesos, de manera que cualquier proceso que tenga problemas puede reiniciarse automáticamente sin afectar los demás procesos activos.

Dirección y administración

Un gran número de avances se han llevado a cabo en las herramientas de administración en Windows Server 2003, entre los que se encuentran:

- En general, se mejora la Consola de Administración de Microsoft, que ahora permite la selección de objetos múltiples para manipulación (cuando sea apropiado) y tiene una interfase gráfica mejorada.
- Se han incorporado al sistema más de 200 nuevos parámetros de política de grupo.
- Windows Server 2003 ahora soporta características de "servidor sin cabeza", con las cuales el servidor puede instalarse y administrarse sin un monitor, teclado o mouse conectado.
- Windows Server 2003 puede actualizarse por sí mismo de manera automática mediante Windows Update. Lo que es más importante, existen ahora Servicios de Actualización de Software de Microsoft que permiten a los administradores bajar y probar actualizaciones de cliente y de servidor antes de asignarlas de forma central a las computadoras del sistema.
- Muchas tareas administrativas se pueden correr ahora desde la línea de comandos. El archivo C:\WINDOWS\HELP\NTCMDS.CHM documenta estas herramientas.

Conectividad de redes

La conectividad de redes es, de hecho, la parte medular de cualquier servidor de red, y el Windows Server 2003 incluye ventajas en sus características de conectividad de redes:

- Se incluye la capacidad IPv6, junto con el soporte de coexistencia para la migración de una red IPv4 a una red IPv6.
- Windows Server 2003 soporta el uso del protocolo punto a punto a través de Ethernet (PPPoE).
- Windows Server 2003 soporta el puenteo de red, en el que se pueden puentear segmentos separados de red a través de un servidor. Esta facilidad puede utilizarse para puentear dos redes similares, como dos segmentos de Ethernet, o aun puentear a través de tipos de redes diferentes, como entre una conexión ISDN conmutada y un adaptador Ethernet en el mismo servidor.
- Se incorporó un firewall de conexión de Internet en Windows Server 2003.

ILUSTRACIÓN DE LAS CARACTERÍSTICAS DE WINDOWS SERVER 2003

El propósito de los capítulos sobre especificaciones del producto de este libro, es familiarizarlo con los productos en cuestión, de manera que usted tenga una idea de las características del producto y de cómo trabajan, y se sienta seguro al conocerlos con detalle, si las llegara a necesitar y cuando las necesite. En esta sección, usted verá algunas de las nuevas características de Windows Server 2003, así como sus pantallas a manera de ilustración.

Tareas del servidor

Windows 2000 Server utiliza el asistente Configure Your Server para facilitar la configuración de un servidor para tareas muy variadas. Windows Server 2003 sigue contando con un asistente llamado Configure Your Server (el cual se encuentra en el menú Administrative Tools), pero ha sido simplificado de manera significativa. La figura 19-1 muestra la pantalla de trabajo principal del nuevo asistente.

Cada opción que se muestra en el asistente Configure Your Server puede seleccionarse a la vez, y cada opción hace que se instale todo el software y las configuraciones necesarias para dicha tarea. Después de que se ha instalado una tarea, usted vuelve a correr el asistente Configure Your Server para seleccionar la siguiente tarea (si la hay) que desea instalar en el servidor y, de hecho, el asistente se reinicia a sí mismo después de que ha terminado cada instalación. Las tareas del servidor disponibles son:

- Servidor de archivos
- Servidor de impresión
- Servidor de aplicaciones (IIS, ASP.NET)
- Servidor de correo (POP3, SMTP)
- Servidor de terminal

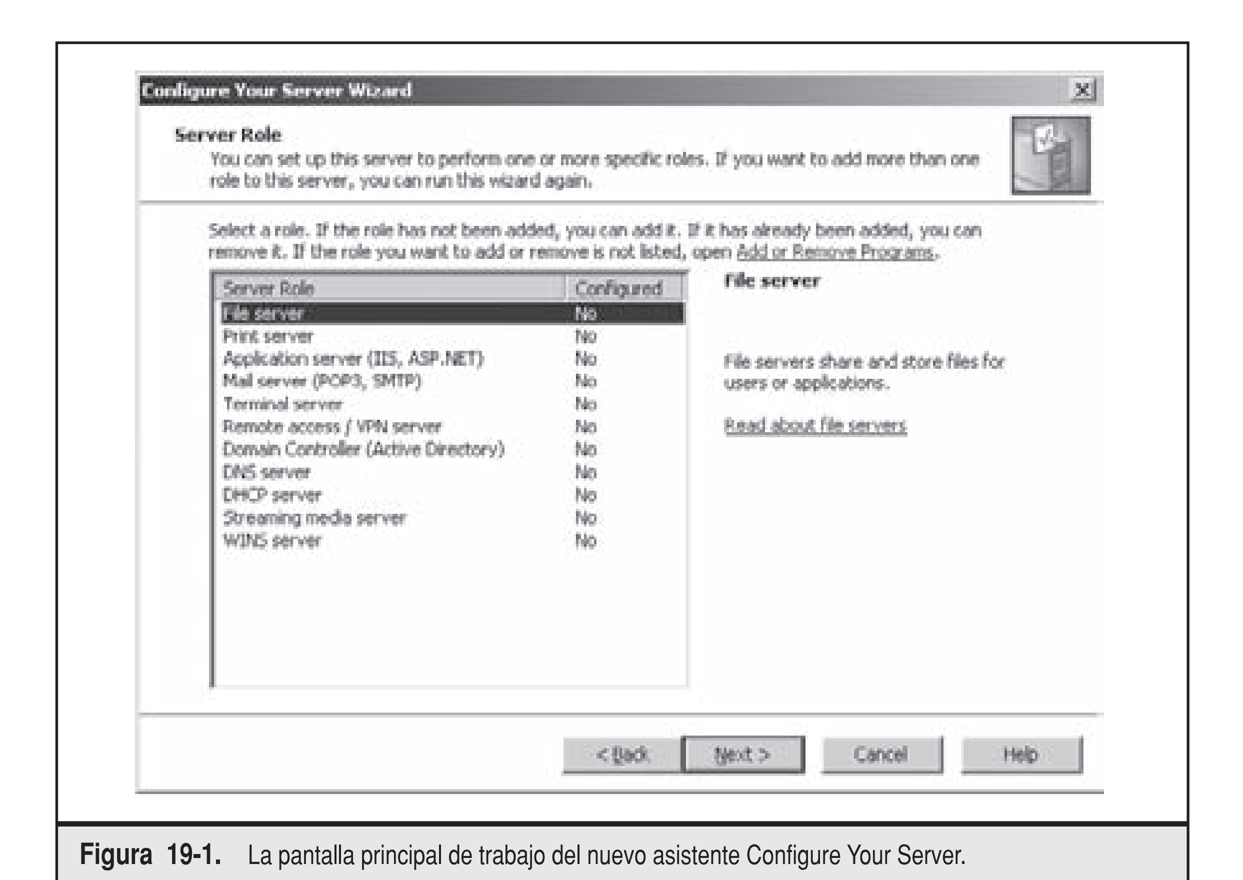


Figura 19-1. La pantalla principal de trabajo del nuevo asistente Configure Your Server.

- Servidor de acceso remoto/ VPN
- Controlador de dominio (directorio activo)
- Servidor DNS
- Servidor DHCP
- Servidor de streaming media
- Servidor WINS

El aspecto más atractivo acerca del nuevo asistente Configure Your Server es que cada tarea seleccionada, cuando se escoja, le solicitará que haga las selecciones que necesite para configurar totalmente esa tarea. Lo anterior hace que la instalación de un servidor con Windows Server 2003 sea muy rápida.

Administración de la web

Windows Server 2003 tiene una nueva capacidad de administración controlada por la web que le permite llevar a cabo muchas tareas de administración del servidor desde una computadora

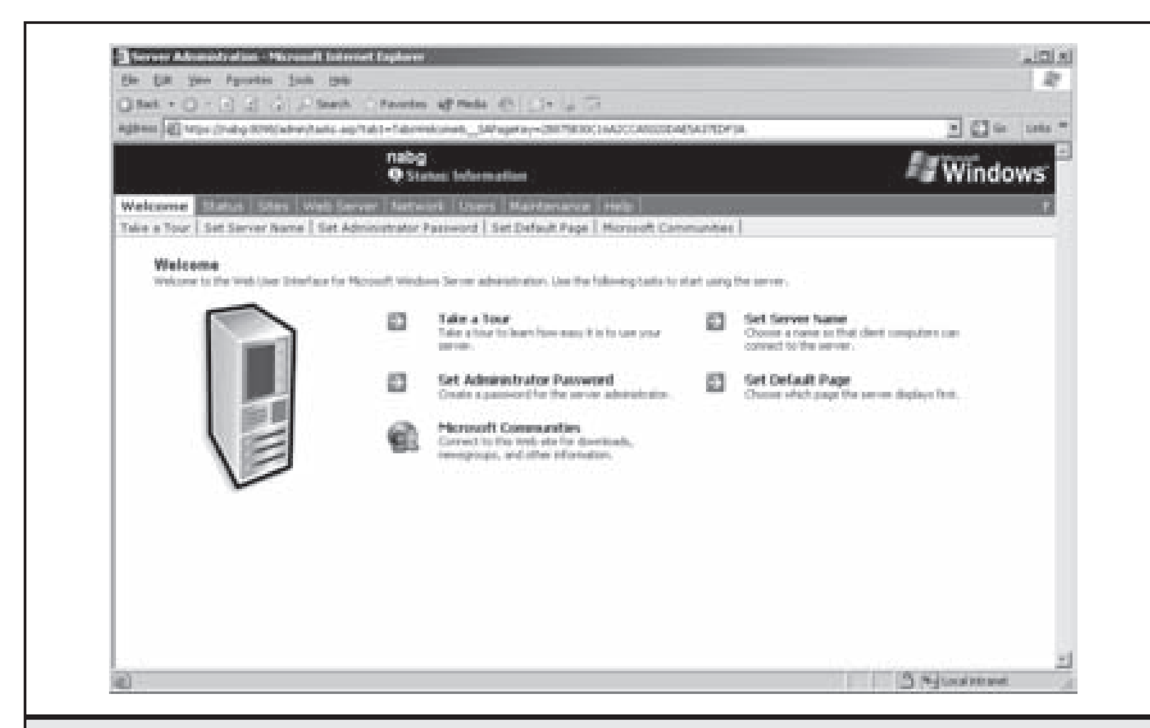


Figura 19-2. Nueva consola de administración remota basada en la web de Windows Server 2003.

remota o local utilizando un navegador web. Puede realizar un arreglo sorprendente de tareas administrativas utilizando la interfase web. La figura 19-2 muestra la pantalla principal de bienvenida de la administración web.

La interfase de administración de la web requiere que se instale el IIS y que corra en el puerto 8098 del servidor. Por ejemplo, si su servidor se llama \\SERVER en su red, entonces la dirección de la administración del web se encontrará en https://server:80998.

Copias de sombra del volumen

Una de las características nuevas más interesantes de Windows Server 2003 se llama Volume Shadow Copies (VSC), que tiene una facilidad correspondiente llamada Volume Shadow Restore. VSC lleva a cabo verificaciones de cambios en los documentos en los volúmenes supervisados. Usted establece los tiempos en los que se realizan y la cantidad de espacio en disco necesario para guardar imágenes VSC. (El valor por omisión es de un máximo de 10 por ciento del volumen). Después, cada vez que se crea una copia de la sombra, se almacena cualquier cambio en los documentos del volumen. Estos cambios almacenados de los documentos pueden ser accesados por los usuarios utilizando la opción de Volume Shadow Restore, la cual permite a un usuario recuperar un archivo eliminado por accidente o regresar a una versión anterior de un archivo, siempre y cuando el documento anterior haya sido capturado por una imagen VSC anterior. Todo esto puede suceder sin que el usuario tenga que solicitar al administrador que recupere los archivos de una cinta, que es lo que típicamente sucede cuando no se cuenta con una ventaja como ésta.

VSC es, de alguna forma, diferente de la característica de salvar archivos de NetWare. Salvar es, en esencia, la capacidad de no eliminar. Sin embargo, en muchos tipos de archivos de documento, la característica de salvar de NetWare le permite recuperar versiones anteriores, debido a la forma en la que la mayoría de los programas salvan archivos. (En general, involucra una eliminación de archivos tras bambalinas, por lo que la opción de salvado puede recuperar versiones anteriores a través de este mecanismo). No obstante, la ventaja de VSC respecto al salvado de NetWare es que funciona con bases de datos y otros tipos de archivos que se modifican en el lugar y también que VSC permite que el programa de respaldo de Windows Server 2003 respalde los archivos que están abiertos mediante el uso transparente de imágenes VSC.

Mejoras en los respaldos

El programa de respaldo incluido en la mayoría de las versiones de varios servidores de Windows puede correrse desde la línea de comando y puede programarse utilizando el servicio de programación junto con el comando AT. Sin embargo, para que un respaldo programado regularmente trabaje de manera apropiada con este método, implica realizar prueba y error hasta encontrar los parámetros adecuados de línea de comandos de msbackup.exe y AT.

El programa de respaldo de Windows Server 2003 incluye una nueva facilidad que hace de la programación de respaldos regulares algo muy rápido. La figura 19-3 muestra la pantalla principal dentro de Backup que le permite establecer una programación.

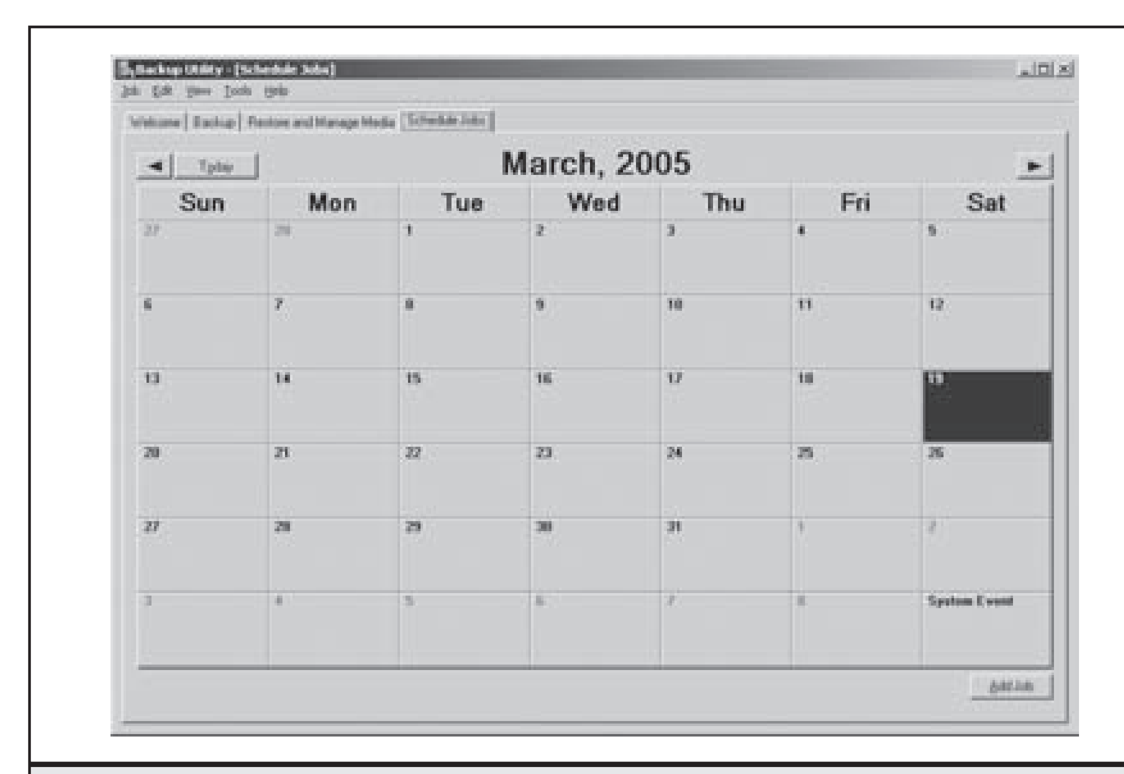


Figura 19-3. La pantalla principal de programación en el programa de respaldo de Windows Server 2003.

Para comenzar una programación de tareas, debe seleccionar el día en el que desea comenzar la tarea, y hacer clic en el botón Add Job. Después, usted será conducido por un asistente que le permitirá definir las propiedades de la tarea de respaldo y, por último, tendrá la oportunidad de establecer la hora y recurrencia de la tarea utilizando las cajas de diálogo estándar con las que se familiarizará.

Otra mejora importante del programa de respaldo es una facilidad llamada recuperación automática del sistema (del inglés automated system recovery, ASR). Los respaldos ASR están diseñados para guardarse en un disco flexible que contenga la información clave que pueda utilizarse para recuperar un sistema de una falla catastrófica del hardware de manera rápida. La figura 19-4 muestra la pantalla inicial del asistente ASR.

Firewall de conexión a Internet

Mientras que muchas organizaciones que cuentan con conexiones de Internet hacia su red tienen dispositivos de firewall dedicados a proteger toda su red, muchas empresas más pequeñas no los tienen. Incluso las empresas que tengan firewalls de red pueden beneficiarse de la incorporación de estos servicios en sus servidores como una medida adicional de prevención. Windows Server

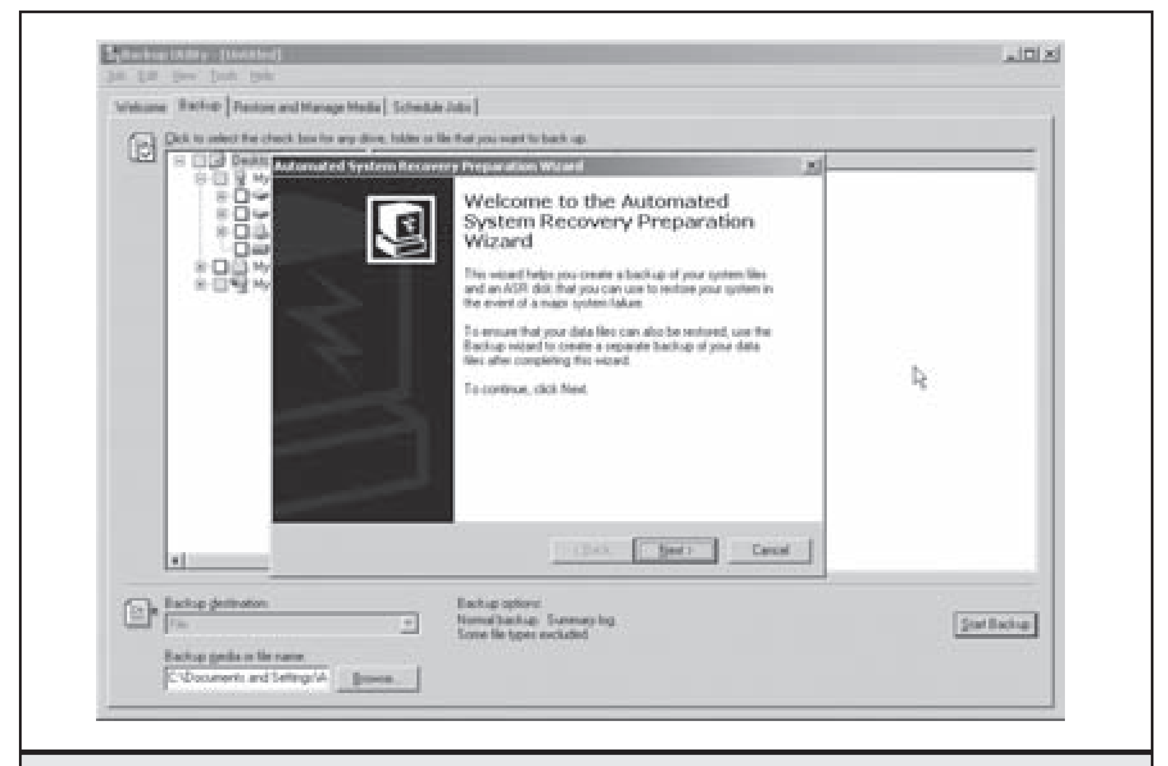


Figura 19-4. La nueva característica ASR le ayuda a recuperarse rápidamente de fallas catastróficas.

2003 incluye un servicio de firewall de inspección de estados muy completo que puede utilizar para proteger el servidor, ya sea como defensa principal o como secundaria. La figura 19-5 muestra dos ventanas de diálogo. En la ventana de diálogo del lado izquierdo, usted habilita firewall (es parte de la ventana de diálogo Properties del objeto de conexión a una LAN), y la ventana del lado derecho es la primero de tres en las que usted define los parámetros de firewall.

La primera de las pestañas de configuración avanzada (que se muestran en el lado derecho de la figura 19-5) le permite seleccionar qué servicios del Windows Server 2003 estarán disponibles para ser accesados a través de su conexión de red. La lista que se desplegará dependerá de qué servicios se encuentran instalados en el servidor. Pueden agregarse nuevos servicios utilizando el botón Add de la pestaña del cuadro de diálogo. Cada uno de los servicios predefinidos ya incluye los puertos IP que el servicio utiliza, mientras que los nuevos servicios que usted agrega en forma manual le permitirán configurar los puertos que deberán protegerse (o permitirse) del servicio.

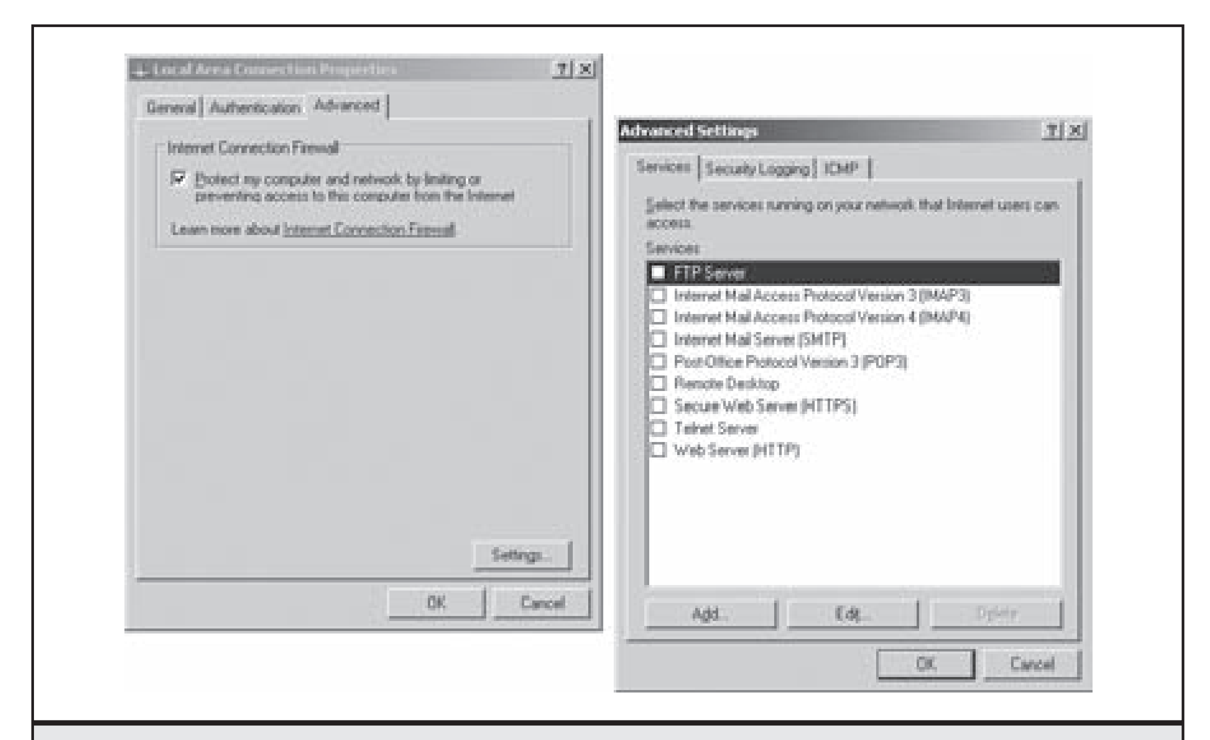


Figura 19-5. Cuando usted habilita firewall de Windows Server 2003, puede acceder a la ventana de diálogo de la firewall Advanced Settings.

La segunda pestaña de la ventana de diálogo Advanced Settings de la firewall (vea la figura 19-6) le permite controlar los parámetros de acceso a ésta. Usted puede seleccionar si desea registrar los paquetes eliminados y las conexiones exitosas (las conexiones que tienen barras siempre se registran), el archivo que se utilizará para almacenar el registro y el tamaño al que puede crecer el registro antes de que sean eliminadas automáticamente las entradas del registro que ingresaron primero.

La pestaña final de la ventana de diálogo Advanced Settings de firewall (vea la figura 19-7) le permite controlar cómo se manejan los paquetes del Internet Control Message Protocol (ICMP). Los puertos ICMP son utilizados por utilidades como PING y son objetivos frecuentes de ataques de negación del servicio. Usted puede seleccionar la entrada de cada tipo de tráfico ICMP, a fin de que pueda leer más acerca de ella, en la parte inferior de la ventana de diálogo. Tenga en mente que puede habilitar ciertos tipos de ICMP de forma temporal para propósitos de reparación y, después, deshabilitar el tipo de tráfico cuando haya terminado la reparación.

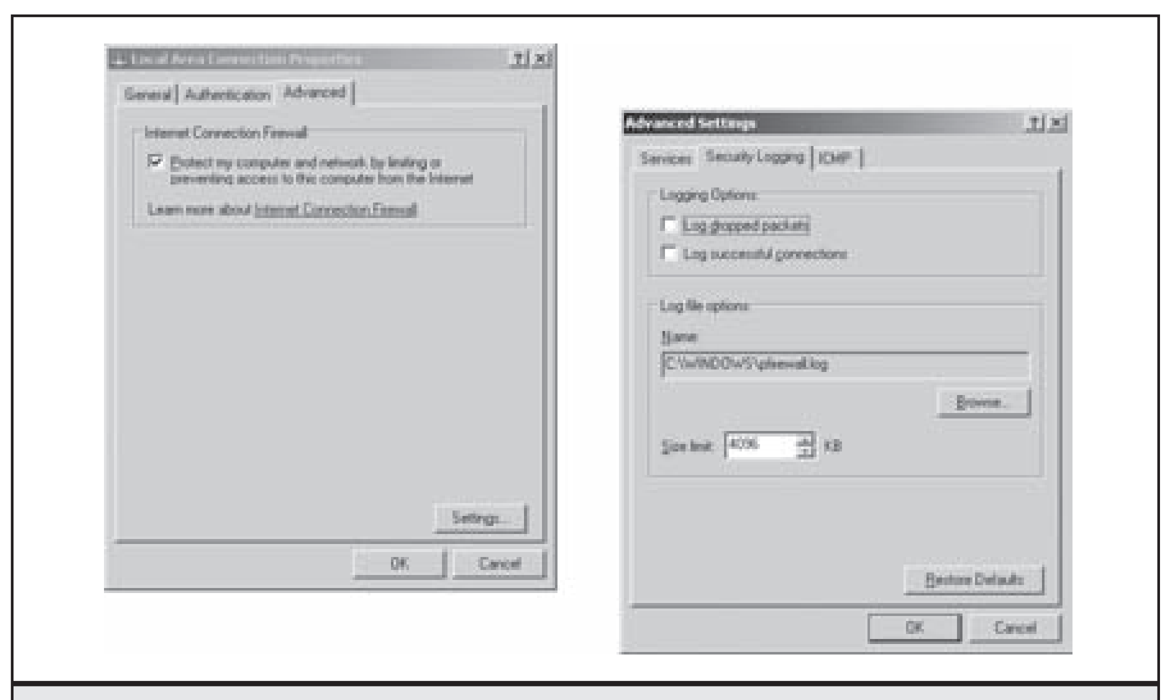


Figura 19-6. La pestaña Security Logging de la caja de diálogo Advanced Settings de firewall.

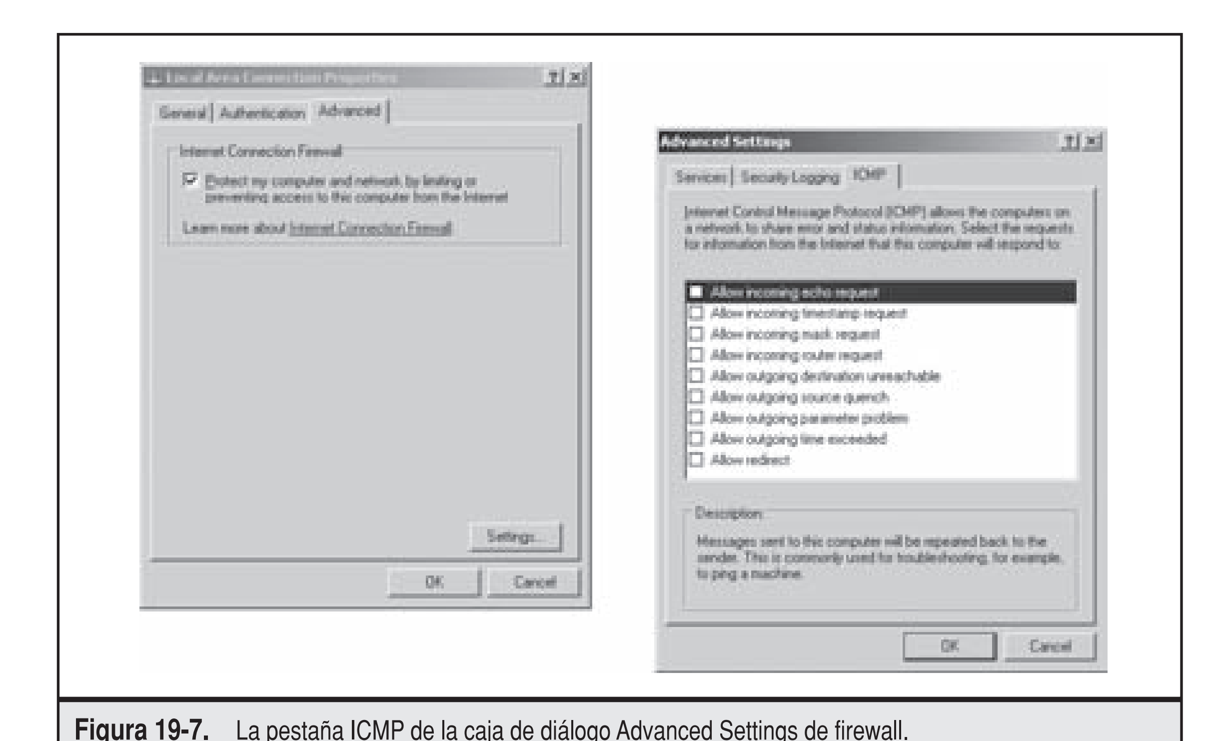


Figura 19-7. La pestaña ICMP de la caja de diálogo Advanced Settings de firewall.

RESUMEN DEL CAPÍTULO

Windows Server 2003 es una actualización muy importante y confiable de Windows 2000 Server. En relación con Windows 2000 Server, se hicieron las mejoras siguientes:

- Más seguridad fuera de la caja.
- Mayor facilidad de administración.
- Mayor facilidad para agregar nuevas tareas a un servidor existente.
- Más confiabilidad.
- Más facilidad para proporcionar servicio.
- Soporte a una mayor cantidad de hardware.

En el capítulo siguiente, usted aprenderá cómo instalar Windows Server 2003 y cómo configurar las características de servidor más comunes que necesitará para construir una red alrededor de un solo sistema Windows Server 2003.



CAPÍTULO 20

Instalación de Windows Server 2003

En este capítulo usted aprenderá cómo instalar Windows Server 2003, lo cual involucra varios pasos, entre los que se encuentran el asegurarse de que el hardware en el que desea hacer la instalación es el adecuado, preparar el servidor y llevar a cabo la instalación. El capítulo siguiente analiza la configuración de una computadora con Windows Server 2003 a fin de brindar los servicios más comunes que se requieren en la red.

EL HARDWARE ADECUADO

Windows Server 2003 requiere un mínimo de hardware. En la mayoría de las ediciones, usted puede instalarlo en computadoras que, de otra forma, utilizaría como estaciones de trabajo. Para aprender acerca de Windows Server 2003, el uso de dicha computadora es totalmente adecuado. Sin embargo, para crear un servidor de producción, estará más a gusto utilizando una computadora diseñada con ese fin. Las computadoras tipo servidor han sido diseñadas y construidas para ser más confiables y proporcionar un mejor servicio que las computadoras de escritorio. Usted puede aprender más acerca de las computadoras tipo servidor en el capítulo 13.

Recuerde del capítulo 19 que existen cuatro ediciones diferentes de Windows Server 2003, algunas de las cuales pueden usarse con procesadores Pentium e Itanium.

Para la edición Web de Windows Server 2003, los niveles de hardware recomendados y mínimos son los siguientes:

- Procesador tipo Pentium (solamente) a una velocidad mínima de 133 MHz. (Microsoft recomienda 550 MHz).
- Al menos 128 MB de RAM. (Microsoft recomienda al menos 256 MB, y yo recomiendo al menos 512 MB).
- Al menos 1.5 GB de espacio disponible en disco duro.

Para la edición Standard:

- Procesador tipo Pentium (solamente) a una velocidad mínima de 133 MHz (Microsoft recomienda al menos 550 MHz). Esta edición puede utilizar hasta 4 procesadores tipo Pentium.
- Al menos 128 MB de RAM. (Microsoft recomienda 256 MB, y yo recomiendo al menos 512 MB). La edición Standard puede utilizar hasta 4 GB de RAM instalada.
- Al menos de 1.25 a 2 GB disponibles de espacio en disco.

Para la edición Enterprise:

- Un procesador tipo Pentium con un mínimo de 133 MHz (se recomiendan 550 MHz). Para un procesador tipo Itanium, un mínimo de 733 MHz. Esta edición puede utilizar hasta ocho procesadores para computadoras que se basen en Pentium o Itanium.
- Al menos 128 MB de RAM instalada. (Yo recomiendo al menos 512 MB). La edición Enterprise puede hacer uso de hasta 32 GB de RAM instalada en computadoras tipo Pentium y 64 GB de RAM instalada en las computadoras tipo Itanium.

- Al menos 1.5 GB de espacio en disco para máquinas tipo Pentium y 2 GB de espacio en disco para máquinas tipo Itanium.

Para la edición Datacenter:

- Ya sea un procesador tipo Pentium a una velocidad mínima de 400 MHz o un procesador tipo Itanium a una velocidad mínima de 733 MHz. La edición Datacenter puede utilizar hasta 64 procesadores para computadoras tanto Pentium como Itanium.
- Un mínimo de 512 MB de RAM (Microsoft recomienda al menos 1 GB de RAM instalada). La edición Datacenter puede utilizar hasta 64 GB de RAM para computadoras Pentium y 512 GB de RAM instalada para computadoras Itanium.
- Al menos 1.5 GB de espacio en disco en máquinas tipo Pentium y 2 GB de espacio en disco en máquinas tipo Itanium.

Después de asegurarse de que el hardware cumpla con los requerimientos mínimos, usted debe confirmar que el hardware específico que planea emplear esté certificado para usarse con Windows Server 2003. Puede hacerlo verificando con el fabricante del hardware que vaya a emplear, o bien, buscando en la Lista de Compatibilidad de Hardware de Microsoft en **http://www.microsoft.com/hcl**. Si usted instala Windows Server 2003 solo para aprender sobre este software, este paso no es tan importante como cuando lo instala para uso masivo.



PISTA Microsoft pone a disposición una edición de evaluación de la edición Enterprise de Windows Server 2003 que puede ocupar para aprender y evaluar el sistema operativo. Puede ordenar la versión de evaluación en un CD-ROM o puede descargarla. Para obtenerla, vaya a **http://www.microsoft.com/windowsserver**, luego navegue en la sección Downloads y, después, en la sección Trial Software Downloads. La versión descargada trabajará durante 180 días y se descarga como una imagen ISO CD-ROM, la mayoría de este software grabable en CD-ROM puede quemarse en un formato listo para operarse, y desde el cual usted podrá instalar el Windows Server 2003.

PREPARAR LA COMPUTADORA DEL SERVIDOR

Es importante que tenga especial cuidado en la preparación del hardware de un servidor de producción. Lo anterior involucra los pasos siguientes:

- Pruebe de manera minuciosa la computadora, utilizando el software de diagnóstico proporcionado por el fabricante. En condiciones óptimas, deberá probar el servidor en un modo de prueba de ciclo sin fin (enless-loop) por un periodo de al menos una semana, aunque dos estaría mejor. A pesar de que el hardware de la computadora es más confiable que nunca, es probable que durante este proceso encuentre alguna parte de la computadora que no está funcionando bien. Las partes más importantes en las que hay que enfocarse son los procesadores, la memoria RAM, las superficies del disco y el controlador.
- Asegúrese de que cuenta con una lista de todos los componentes instalados en el servidor.

▲ Verifique que tiene disponible el controlador de los CD-ROM proporcionados por el fabricante. Muchas veces, durante la instalación de Windows Server 2003, es probable que éste no soporte algunos componentes sin instalar antes algún controlador en particular, quizá para el controlador del disco o las tarjetas de red. Asimismo, muchos fabricantes proporcionan rutinas de instalación especiales que automáticamente instalan cualquier tipo de controlador necesario como parte de la instalación de Windows Server 2003. Cuando dicha rutina se encuentre disponible, usted deberá utilizarla.



NOTA El capítulo 16 estudia con más detalle la preparación del hardware del servidor como parte de la instalación de Windows 2000 Server. Los pasos preparatorios que debe realizar son los mismos en ambos sistemas operativos, por lo que deberá revisar ese material a fin de encontrar más detalles acerca de las tareas de preinstalación.

INSTALACIÓN DE WINDOWS SERVER 2003

Windows Server 2003 puede instalarse utilizando el CD-ROM proporcionado o, en algunos casos, a través de una conexión con la ayuda de un servidor fuente para la instalación preparada de forma especial. Sin embargo, a menos que emplee muchas computadoras con Windows Server 2003, la instalación con el CD-ROM es lo que debe utilizar y es lo que se muestra aquí.

Una vez que ha terminado todos los preparativos, puede comenzar el proceso de instalación reiniciando la computadora desde el CD-ROM de Windows Server 2003. La instalación comienza en modo de texto y carga primero todo el software de soporte al hardware necesario, lo cual toma un minuto o dos; después, ve la pantalla Welcome To Setup que se muestra en la figura 20-1.

En la pantalla Welcome, puede presionar ENTER para iniciar la instalación o la tecla R para reparar una instalación existente de Windows Server 2003. Puesto que estamos instalando desde el inicio, presione la tecla ENTER para continuar.

A continuación se le presenta el acuerdo de licencia de Windows Server 2003. Para aceptar el acuerdo, presione F8.

Luego se le muestra una lista de dispositivos de disco disponibles con los que puede instalarse Windows Server 2003, como se muestra en la figura 20-2. En esta pantalla, también puede crear y eliminar particiones en el disco, si fuera necesario. Para eliminar una partición existente, presione la tecla D; para crear una nueva partición en un espacio no dividido, presione la tecla C.

En este ejemplo, se necesita crear una partición en el disco, por lo que tendría que presionar la tecla C. Esto trae la pantalla de crear una partición que se muestra en la figura 20-3. En este ejemplo, se utilizará el disco completo, así que acepte la creación por omisión de una partición de 8 GB en el disco de 8 GB presionando ENTER.

Realizar la partición lo lleva de regreso a la pantalla de selección de partición, que se muestra en la figura 20-4. Si necesita crear particiones adicionales, puede hacerlas en este punto. Puesto que este ejemplo solo se ocupa de una partición, la barra resaltada se mueve hacia dicha partición. Presione ENTER para seleccionar esa partición y continuar.

```
Windows Server 2003, Enterprise Edition Setup

  Welcome to Setup.

  This portion of the Setup program prepares Microsoft(R)
  Windows(R) to run on your computer.

      •  To set up Windows now, press ENTER.

      •  To repair a Windows installation using
         Recovery Console, press R.

      •  To quit Setup without installing Windows, press F3.

  ENTER=Continue  R=Repair  F3=Quit
```

Figura 20-1. La pantalla Welcome to Setup es el punto de partida de la instalación de Windows Server 2003.

```
Windows Server 2003, Enterprise Edition Setup

  The following list shows the existing partitions and
  unpartitioned space on this computer.

  Use the UP and DOWN ARROW keys to select an item in the list.

      •  To set up Windows on the selected item, press ENTER.

      •  To create a partition in the unpartitioned space, press C.

      •  To delete the selected partition, press D.

  8190 MB Disk 0 at Id 0 on bus 0 on symmpi (MBR)

      Unpartitioned space                    8189 MB

  ENTER=Install  C=Create Partition  F3=Quit
```

Figura 20-2. Seleccione una partición en la cual se instalará Windows Server 2003.

```
Windows Server 2003, Enterprise Edition Setup

You asked Setup to create a new partition on
8190 MB Disk 0 at Id 0 on bus 0 on symmpi [MBR].

  •  To create the new partition, enter a size below and
     press ENTER.

  •  To go back to the previous screen without creating
     the partition, press ESC.

The minimum size for the new partition is     8 megabytes (MB).
The maximum size for the new partition is  8182 megabytes (MB).
Create partition of size (in MB):  8182

ENTER=Create  ESC=Cancel
```

Figura 20-3. Creación de una partición en la ventana Setup.

```
Windows Server 2003, Enterprise Edition Setup

The following list shows the existing partitions and
unpartitioned space on this computer.

Use the UP and DOWN ARROW keys to select an item in the list.

  •  To set up Windows on the selected item, press ENTER.

  •  To create a partition in the unpartitioned space, press C.

  •  To delete the selected partition, press D.

8190 MB Disk 0 at Id 0 on bus 0 on symmpi [MBR]

    C:  Partition1 [New (Raw)]             8182 MB (  8181 MB free)
        Unpartitioned space                   8 MB

ENTER=Install  D=Delete Partition  F3=Quit
```

Figura 20-4. Seleccionar una partición en la cual se instalará Windows Server 2003.

Después de seleccionar la partición, se le pregunta el método que se utilizará para formatear la partición (vea la figura 20-5). Para Windows Server 2003, recomiendo siempre seleccionar NTFS. Seleccione Format the Partition Using the NTFS File System, y presione ENTER.

La partición se formatea ahora. El programa Setup examina el disco a fin de encontrar algún problema y, después, copia de forma automática todos los programas de instalación de gráficos a la nueva partición. Al final de este proceso, el sistema se reinicia y el proceso de instalación continúa en modo gráfico. La mayor parte del proceso de instalación de gráficos corre automáticamente y requiere muy poca ayuda de usted conforme el proceso se desarrolla. El comienzo de la fase gráfica se muestra en la figura 20-6.

Lo primero que se le solicita en la instalación de gráficos es establecer las opciones de región e idioma. En general, éstas ya están fijas por omisión en el país donde reside; sin embargo, si fuere necesario, puede modificar estos parámetros utilizando el botón Customize que se muestra en la figura 20-7. Si los valores por omisión son correctos, haga clic en Next para continuar.

A continuación se le solicita ingresar su nombre y el de su organización. Recomiendo que solo escriba el nombre de su compañía en ambos campos. De cualquier forma, ingrese la información apropiada y presione Next para continuar.

Luego se le pide que ingrese el número de serie. Si está instalando la edición de evaluación de Windows Server 2003, dicho número se le deberá enviar por correo electrónico. De otra forma, puede localizarlo en la caja del CD de Windows Server 2003 o, a veces, en una calcomanía colo-

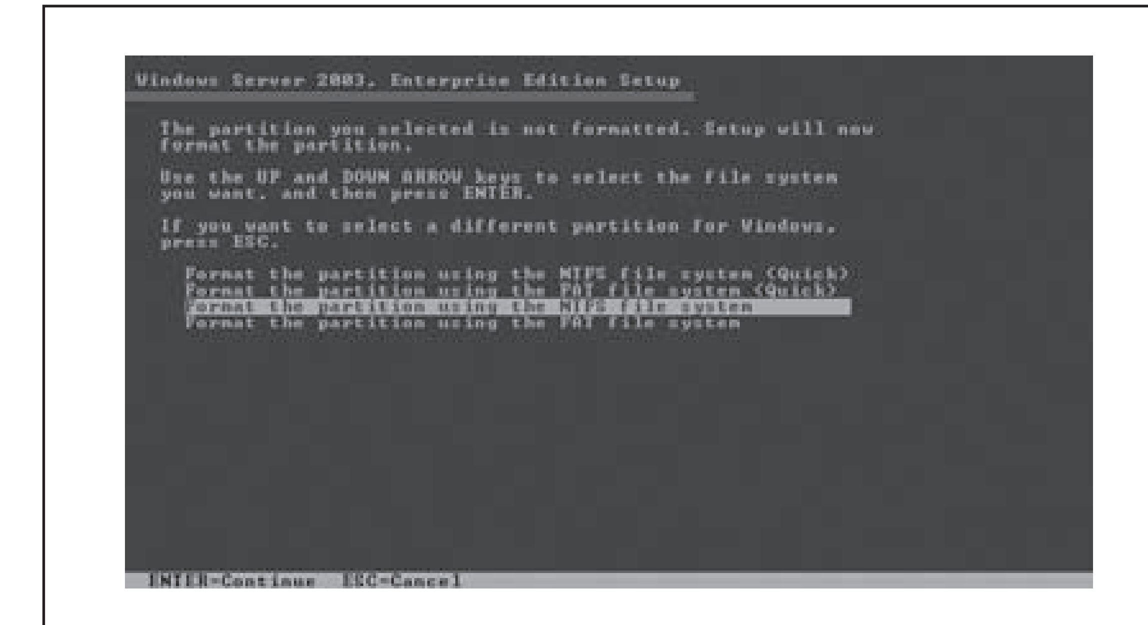


Figura 20-5. Seleccionar el formato del disco de la partición instalada.



Figura 20-6. El inicio de la porción gráfica del proceso de instalación.

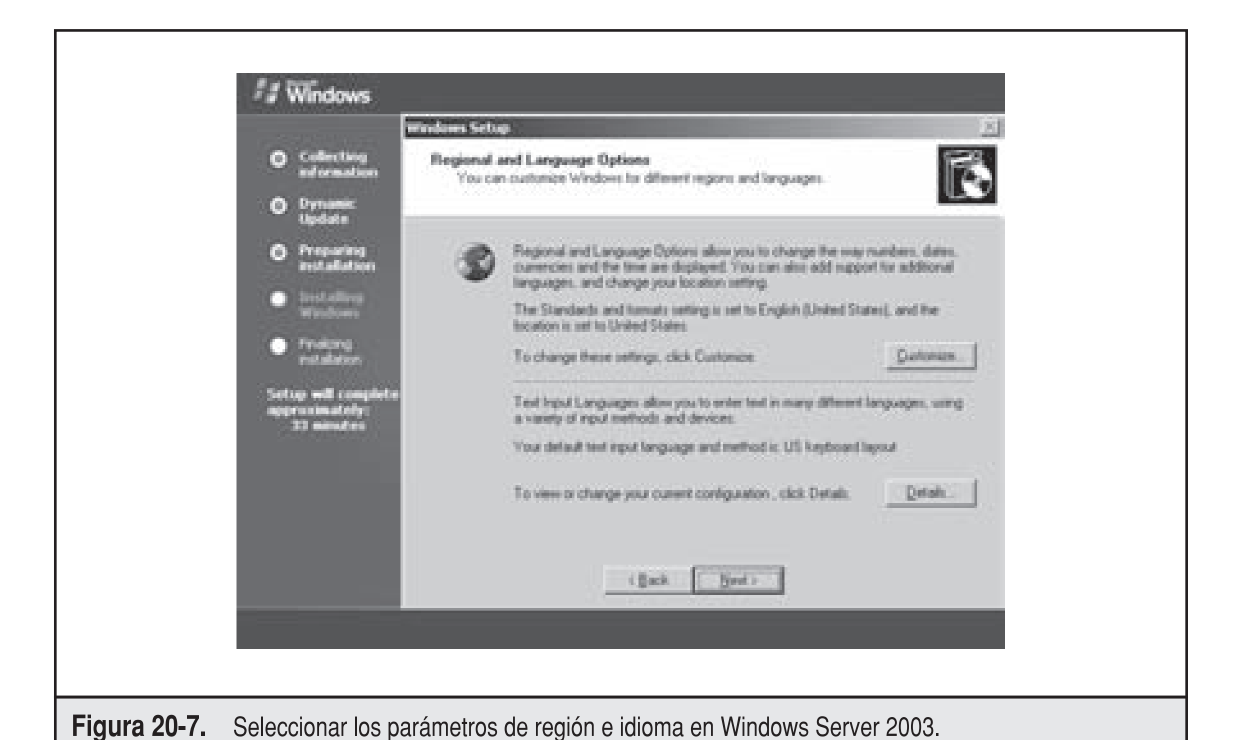


Figura 20-7. Seleccionar los parámetros de región e idioma en Windows Server 2003.

cada en la computadora que está utilizando, si es que fue adquirida con una copia de Windows Server 2003. Ingrese la tecla apropiada y seleccione Next para continuar.

Después, se le solicitará que seleccione el modo de licencia de su servidor, y puede escoger ya sea Per Server, Per Device o Per User. Para un servidor de evaluación, seleccione Per Device o Per User y haga oprima Next para continuar.

NOTA Véase la sección titulada "¿Por sitio o por servidor?", del capítulo 16, para encontrar más información acerca de las diferencias entre estos dos modos de licencia.

A continuación se le solicitará proporcionar el nombre del servidor, así como asignar una contraseña para la cuenta administrativa local, como se muestra en la figura 20-8. Ingrese un nombre para el servidor y seleccione e ingrese una contraseña administrativa también. Haga clic en Next para continuar.

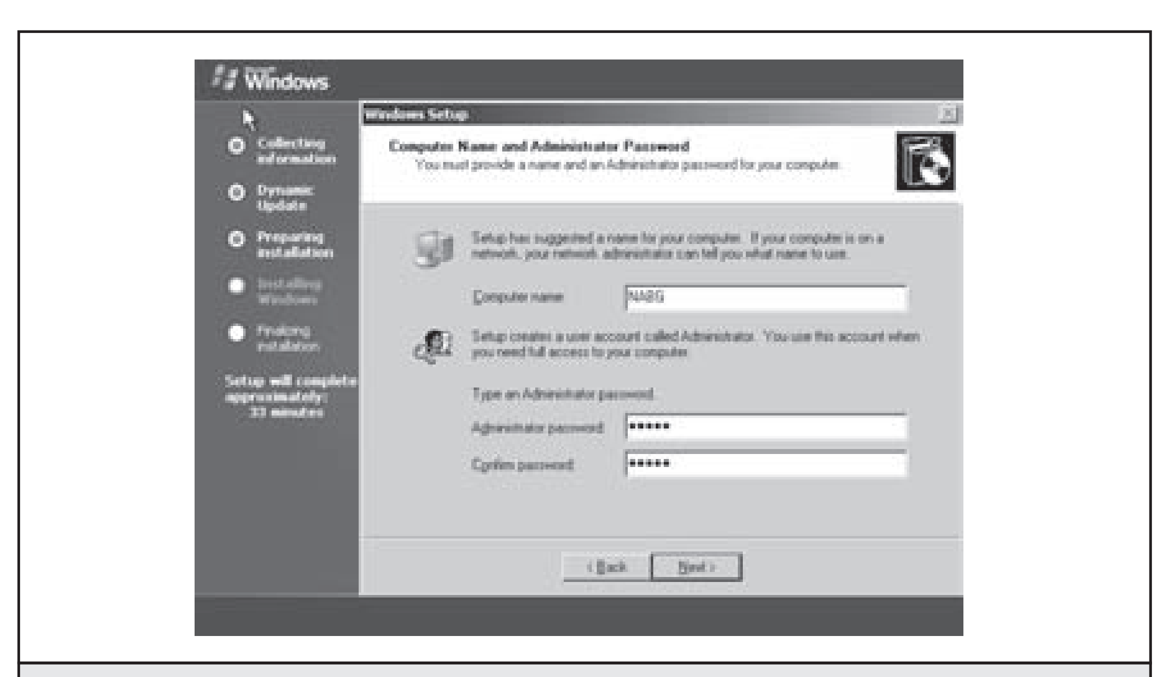


Figura 20-8. Escoger un nombre y una contraseña administrativa para el servidor.

Posteriormente, se le solicitará seleccionar su huso horario y confirmar que la fecha y la hora del servidor sean correctas. Haga clic en Next para continuar. El software de soporte de la conectividad de redes está ahora instalado y, en la pantalla que se muestra en la figura 20-9, se le solicitará seleccionar los parámetros de conectividad de redes para el servidor.

En la mayoría de las instalaciones de servidores, usted establece una dirección IP fija en lugar de utilizar una dirección proporcionada por el DHCP. En particular, cuando está configurando un nuevo servidor en una red, tendrá que hacer lo anterior, ya que el DHCP no existirá todavía en la red. También es muy común que quiera que los servidores cuenten con una dirección IP que no cambie, la cual es otra razón para que les fije una dirección determinada. Para hacer esto, haga clic sobre el botón Custom Settings y, luego, sobre el botón Next, el cual hace que aparezca la ventana de diálogo Networking Components que se muestra en la figura 20-10.

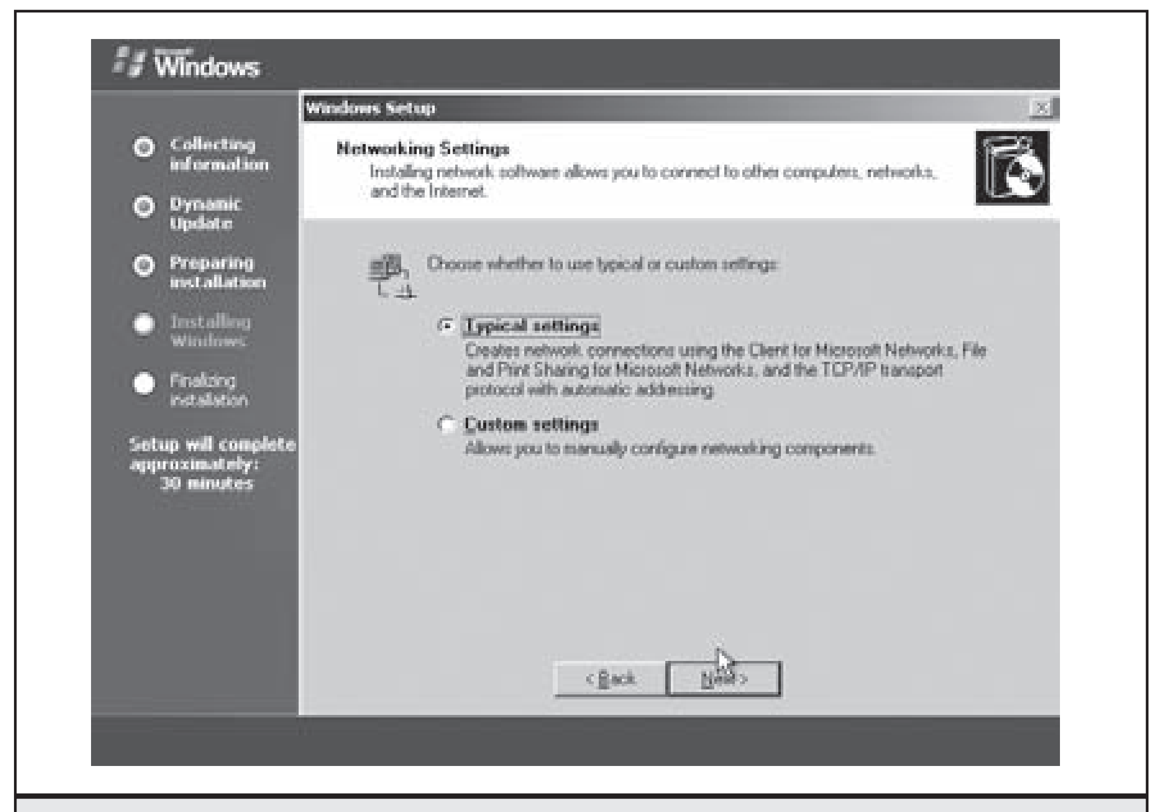


Figura 20-9. Seleccionar los parámetros de la conectividad de redes.

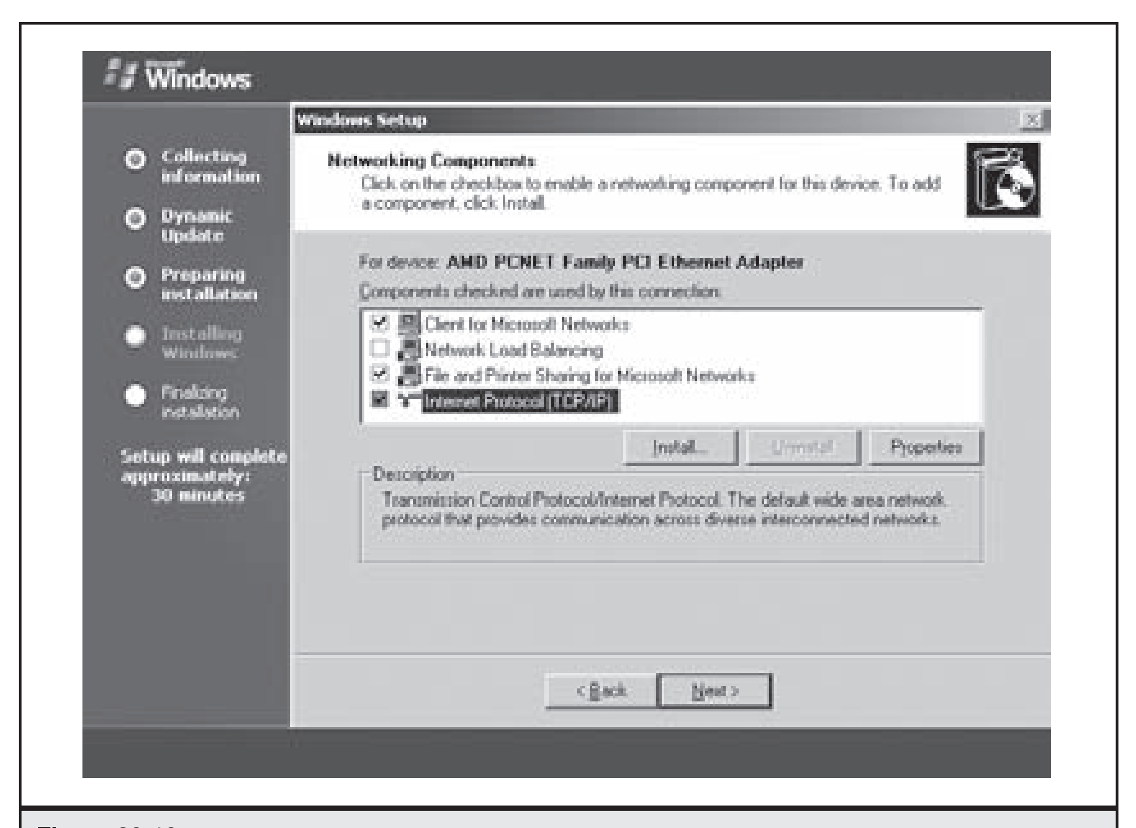


Figura 20-10. Definir los componentes de la conectividad de redes.

En la ventana de diálogo Networking Components, seleccione la opción Internet Protocol (TCP/IP) y presione el botón Properties, lo que trae al frente la ventana Protocol (TCP/IP) Properties, que se muestra en la figura 20-11, en la que usted puede asignar la dirección IP, la máscara de subred y la dirección por omisión de la compuerta que se utilizará para el servidor. Ingrese los parámetros apropiados de su red y haga clic en OK para cerrar la ventana de diálogo y, después oprima Next para continuar la instalación.

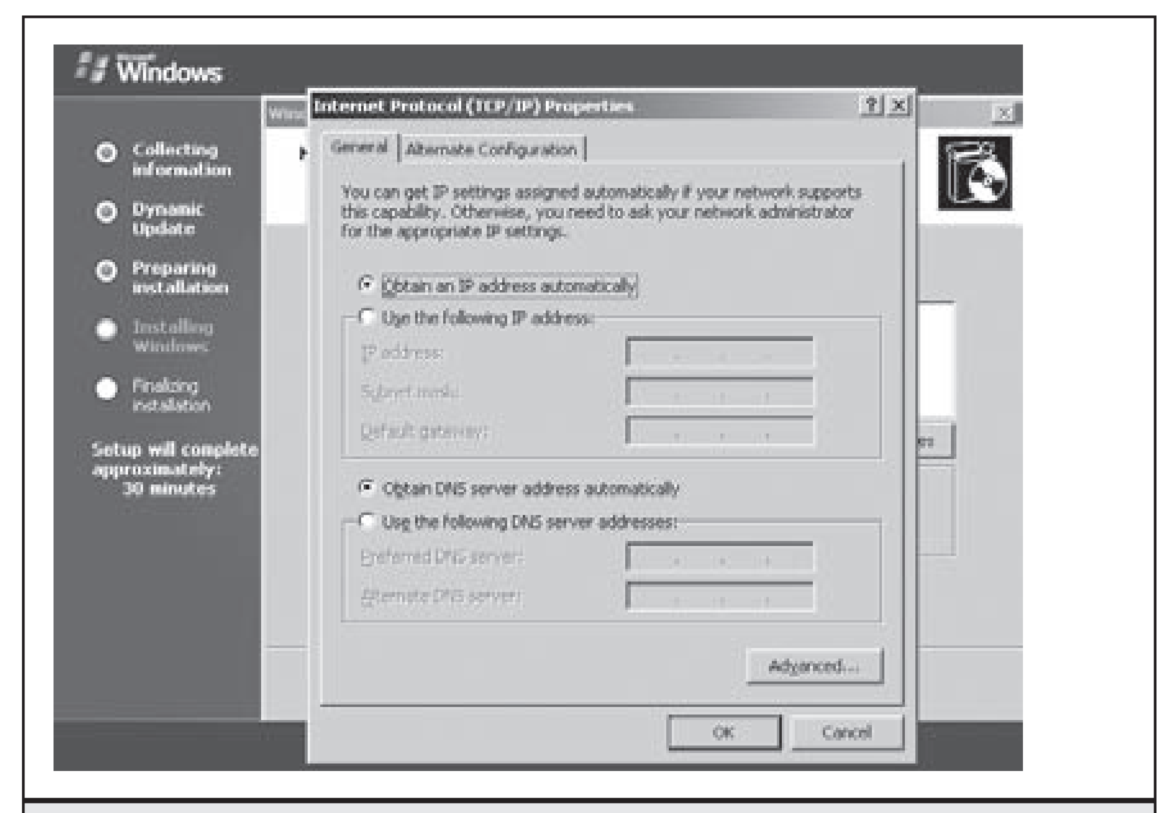


Figura 20-11. Establecer una dirección IP fija durante la instalación.

A continuación, se le solicita que seleccione un grupo de trabajo al cual le asignará el servidor o, si existe un dominio trabajando, puede agregar este servidor al dominio (figura 20-12). Si configura el servidor como primer servidor e intenta hacerlo un controlador de dominio, entonces debe seleccionar Workgroup, por lo pronto. De otra forma, seleccione un dominio existente; si selecciona esta opción, necesitará el nombre de la cuenta y la contraseña de una cuenta que tenga la facultad de agregar computadoras al dominio.

Por último, la instalación se termina de forma automática, después la computadora se reinicia. En general, este proceso de finalización toma aproximadamente 20 minutos. Después de que éste ha terminado, el servidor se reinicia de manera automática, y puede entrar utilizando el nombre de usuario Administrator y la contraseña administrativa que asignó durante el proceso de instalación.

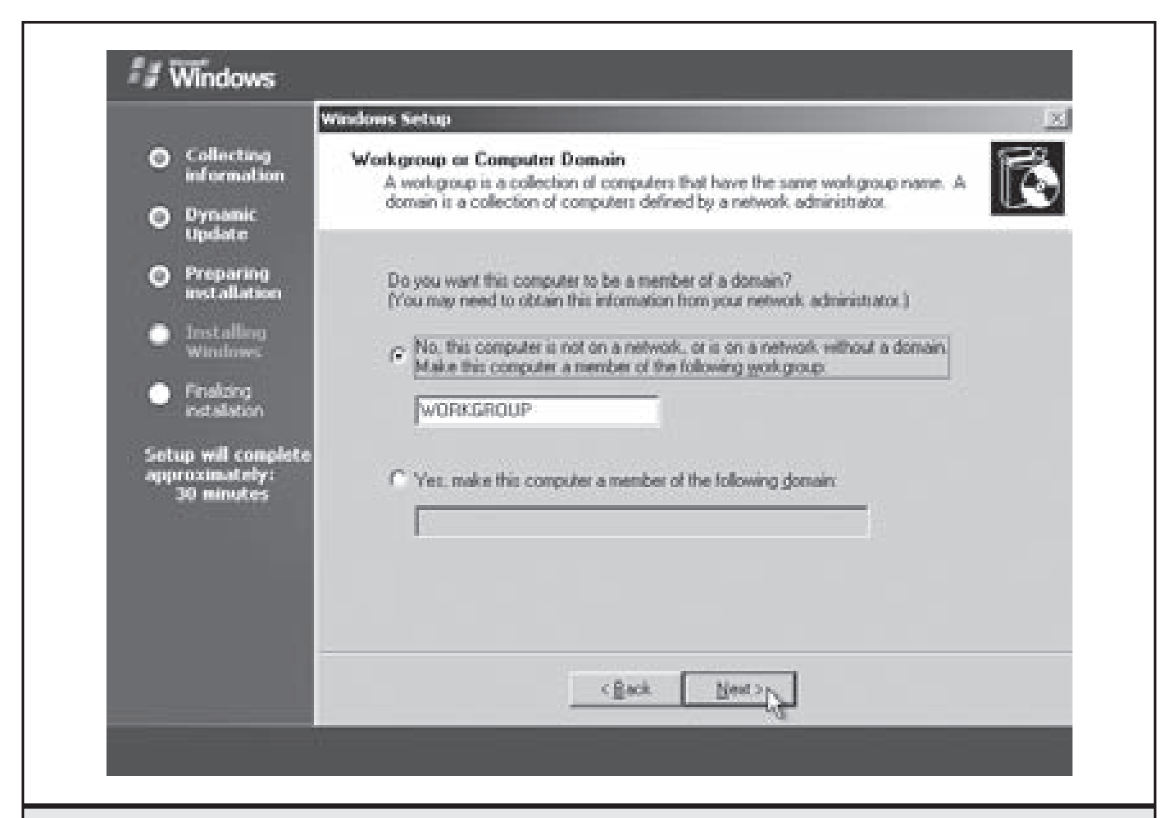


Figura 20-12. Seleccionar membresía de grupo de trabajo o de dominio.

RESUMEN DEL CAPÍTULO

En este capítulo usted aprendió cómo prepararse e instalar Windows Server 2003. Como pudo estudiar, el proceso de instalación es relativamente automático y fácil de seguir, y no le proporciona opciones para instalar servicios y facilidades adicionales, como lo hace cuando instala Windows 2000 Server. En lugar de lo anterior, Windows Server 2003 le permite agregar fácilmente servicios y características adicionales después de haber sido instalado. El capítulo 21 le enseñará cómo hacer esto para algunos servicios comunes que necesitará en la mayoría de las redes.



CAPÍTULO 21

Configuración de Windows Server 2003

El capítulo 20 le enseñó qué tan directa es la instalación de Windows Server 2003; en parte porque muchas tareas no se llevan a cabo durante ésta, sino que se realizan en la postinstalación del servidor. Este capítulo le enseña cómo instalar y configurar una gran cantidad de servicios comunes del servidor de red.

Después de terminar la instalación de Windows Server 2003, el sistema se reinicia y, luego, le permite tener acceso a él utilizando el número de cuenta del administrador y la contraseña que usted ingresó en la instalación. Después de teclear éste e ingresar al sistema, usted verá la ventana Manage Your Server que se muestra en la figura 21-1.

En versiones anteriores de servidores Windows, tenía que conocer qué componentes de software instalar a fin de llevar a cabo diferentes tareas. Windows Server 2003 es mucho más sencillo en este sentido. Ahora, simplemente tiene que agregar "tareas" al servidor.

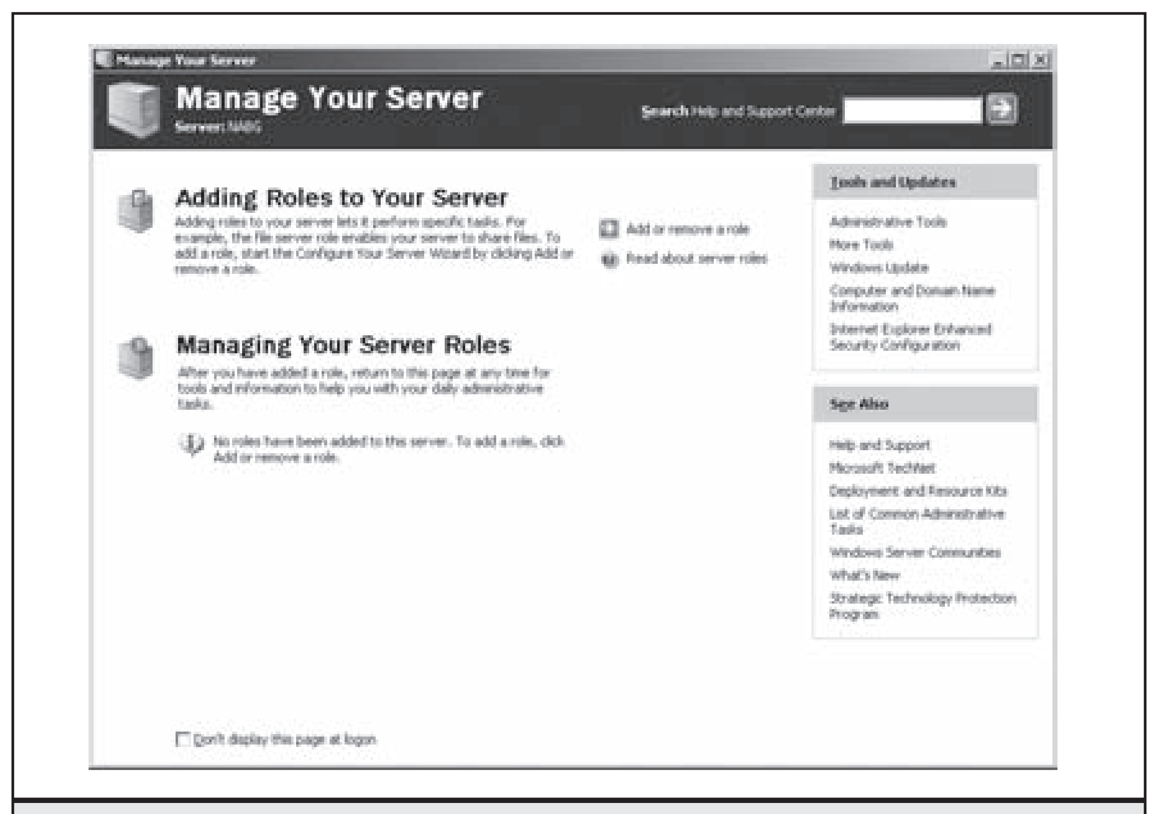


Figura 21-1. La ventana Manage Your Server.

Figura 21-2. El asistente Configure Your Server le permite agregar fácilmente tareas a un servidor.

La aplicación Manage Your Server instala todo el software necesario para que las tareas estén disponibles a través del asistente Configure Your Server Wizard, que se muestra en la figura 21-2.

Las secciones restantes de este capítulo analizan las tareas más comunes que usted deseará configurar en Windows Server 2003.

CREAR UN CONTROLADOR DE DOMINIO

Una de las primeras tareas que deben configurarse en una red nueva es la del controlador de dominio, el cual maneja las solicitudes del directorio activo y sirve como un depósito de toda la información relativa al directorio y a la seguridad de la red.



NOTA El capítulo 9 estudia con más detalle el directorio activo (AD) y sus capacidades.

En el Configure Your Server Wizard, seleccione Domain Controller (Active Directory) y presione Next para continuar. Después verá el Active Directory Installation Wizard, que se muestra en la figura 21-3.



PRECAUCIÓN Si está instalando Windows Server 2003 en una red existente, sea extremadamente cuidadoso respecto a configurar un servidor de evaluación como controlador de dominio. En realidad, esto no se recomienda; en lugar de eso, deberá poner el servidor de evaluación en su propia red, en la cual podrá configurar el servidor de evaluación como un controlador de dominio para uno nuevo.

Después de observar una pantalla que le advertirá que Windows 95 y Windows NT 4 no pueden hacer uso total de los dominios del directorio activo, se le da la opción entre instalar un controlador de dominio para un dominio nuevo o agregar un controlador de dominio a uno existente (vea la figura 21-4). En este ejemplo, usted creará un nuevo dominio. Seleccione esa opción y haga clic en Next para continuar.

A continuación, se le solicita información respecto a qué tipo de dominio va a crear, como se muestra en la figura 21-5. En este ejemplo, usted creará un bosque nuevo, en vez de crear un dominio hijo o un nuevo árbol dentro de un bosque existente. Así que seleccione Domain in a new forest y haga clic en Next para continuar.



Figura 21-3. Comienzo de la instalación de un controlador de dominio a través del Active Directory Installation Wizard.

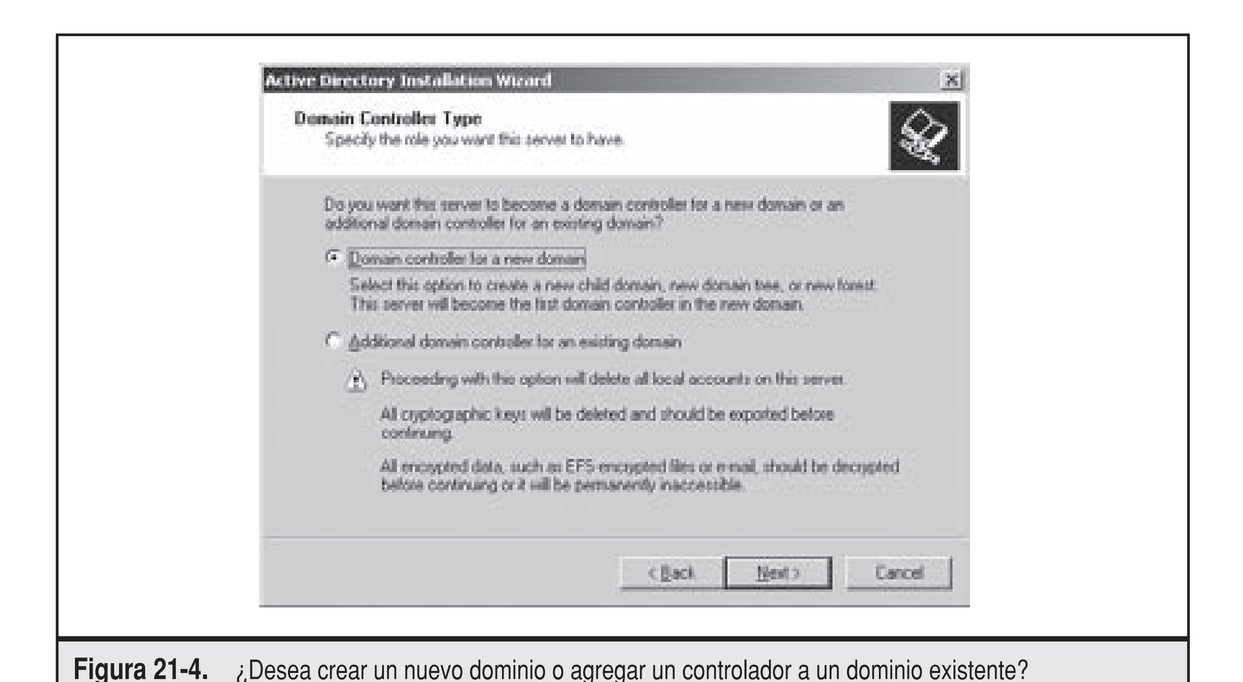


Figura 21-4. ¿Desea crear un nuevo dominio o agregar un controlador a un dominio existente?

Figura 21-5. Seleccionar qué tipo de dominio crear.

Luego se le invita a ingresar el nombre del nuevo dominio, como en la figura 21-6. En este ejemplo, se creará un dominio llamado nabg.org (NABG viene del inglés Networking: A Beginners's Guide [Conectividad de redes: una guía para el principiante]). Por supuesto, usted puede seleccionar cualquier nombre de dominio que desee utilizar.

Después, se le solicitará asignar un nombre de NetBIOS al servidor de la red (figura 21-7). Con mucha frecuencia, el asistente de instalación asignará un nombre basado en el de la computadora; sin embargo, si fuera necesario, puede cambiar el nombre de NetBIOS aquí. Haga clic en Next para continuar.

Ahora se le pide que proporcione una ubicación en el disco, donde desea que se almacene la base de datos del directorio activo y los registros, como se muestra en la figura 21-8. La mejor opción aquí es aceptar la ubicación que se muestra por omisión y presionar Next para continuar.

En el siguiente paso, se le pide la ubicación en la que se almacenará la copia de los archivos del dominio público del servidor. La ubicación por omisión es C:\WINDOWS\SYSVOL, la cual también le recomiendo que mantenga. Oprima Next para continuar.

Enseguida, el asistente de la instalación realizará pruebas en el servidor DNS que ha sido configurado en las propiedades TCP/IP del servidor. El director activo depende del DNS para almacenar cosas, como los nombre de los servidores de la red. Usted siempre debe tener un servidor DNS local para cualquier dominio que administre. De acuerdo con esto, cuando vea esta pantalla (suponiendo que no cuenta con un servidor DNS en su red de prueba), deberá

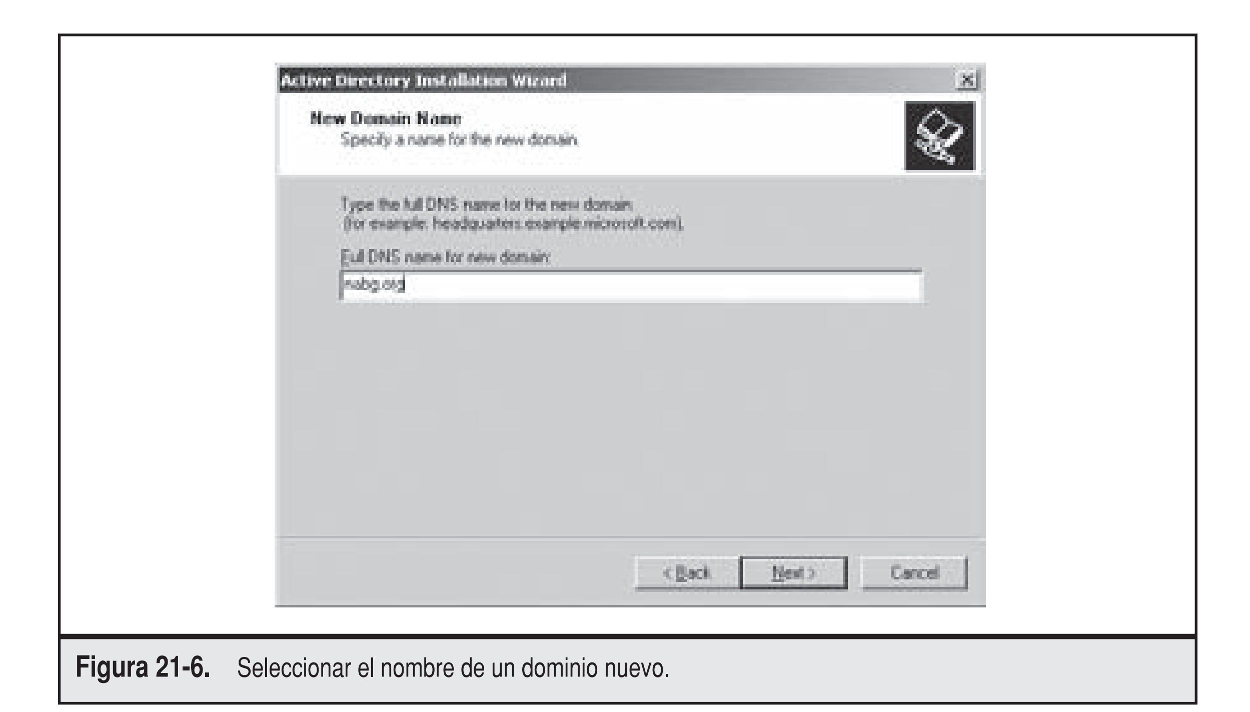


Figura 21-6. Seleccionar el nombre de un dominio nuevo.



Figura 21-7. Asignar un nombre NetBIOS.

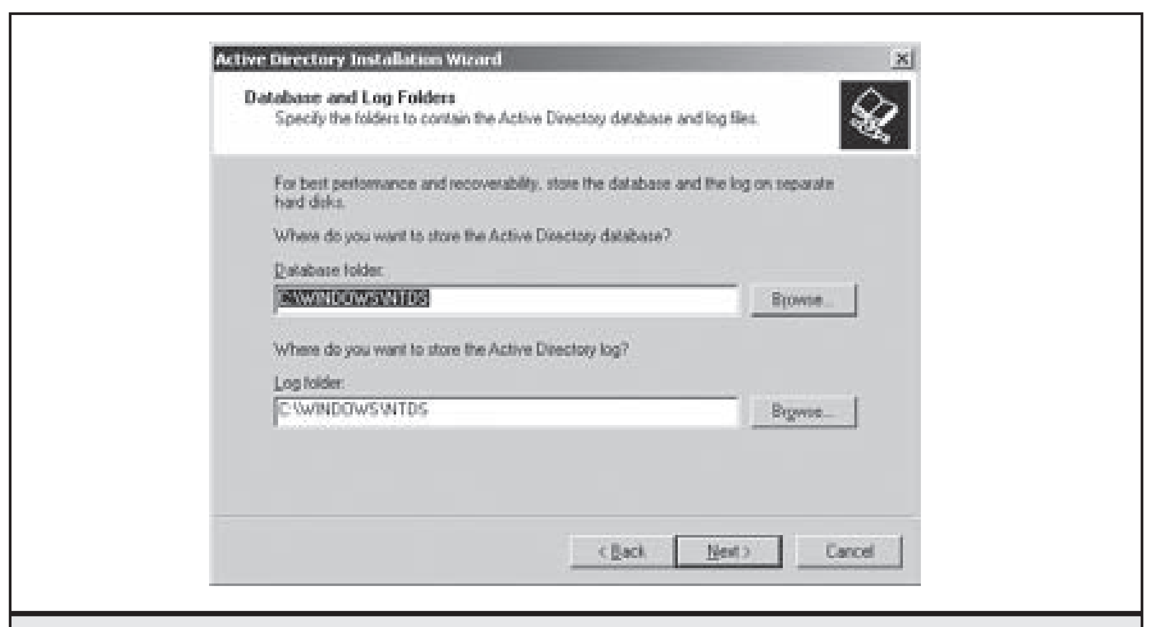


Figura 21-8. Localizar la base de datos del Directorio Activo y los registros.

seleccionar la segunda opción: Install and configure the DNS server on this computer, y hacer clic en Next para continuar. La figura 21-9 muestra la pantalla de diagnóstico que verá.

A continuación, se le solicitan los estilos de permisos por omisión que se utilizarán en el nuevo dominio (vea la figura 21-10). Usted puede seleccionar que se dé soporte a un dominio preWindows 2000 Server o un dominio que solamente soporte controladores de Windows 2000 Server y Windows Server 2003. Seleccione la opción indicada y haga clic en Next para continuar.

Enseguida se le solicita asignar una contraseña de modo de recuperación para el directorio activo, la cual le será útil si en algún momento necesita recuperar el directorio activo. La contraseña del modo de recuperación es para una cuenta de administrador diferente a la cuenta Administrator normal del servidor, así que almacene esta contraseña en un lugar seguro. La figura 21-11 muestra esta caja de diálogo.

Por último, observará una pantalla de resumen que le permitirá revisar todas sus selecciones antes de que se cree el dominio. Usted deberá verificar esta pantalla y, después, presionar el botón Next para terminar la instalación. Es probable que se le pida su CD-ROM de Windows Server 2003 durante la instalación. Al final de ésta, el servidor se reiniciará.

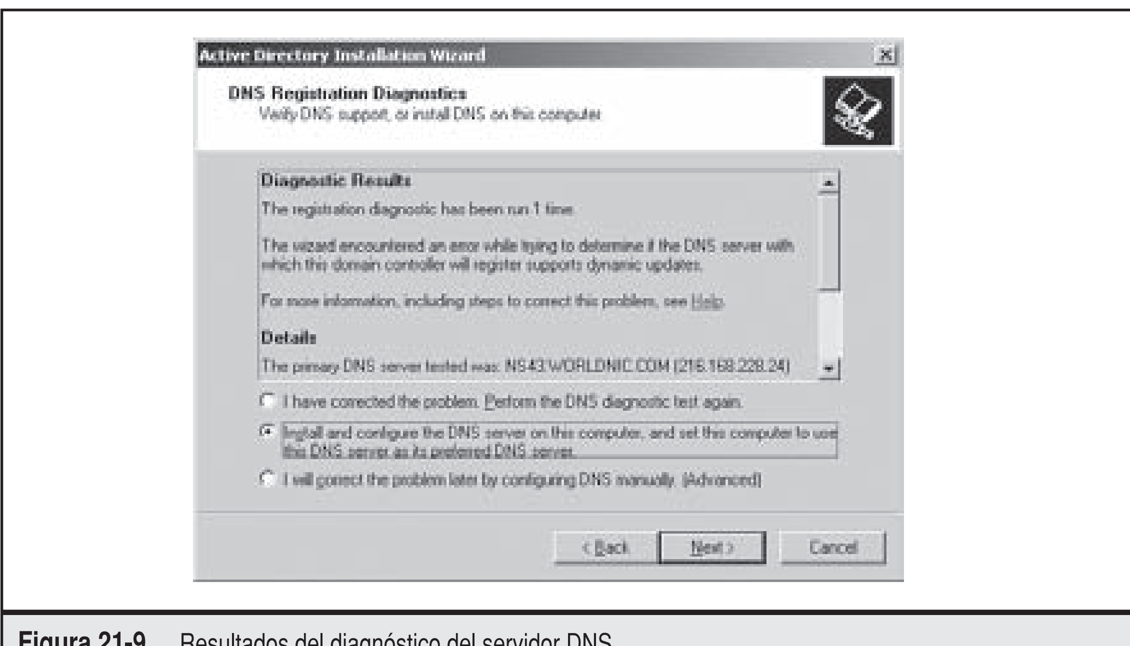


Figura 21-9. Resultados del diagnóstico del servidor DNS.

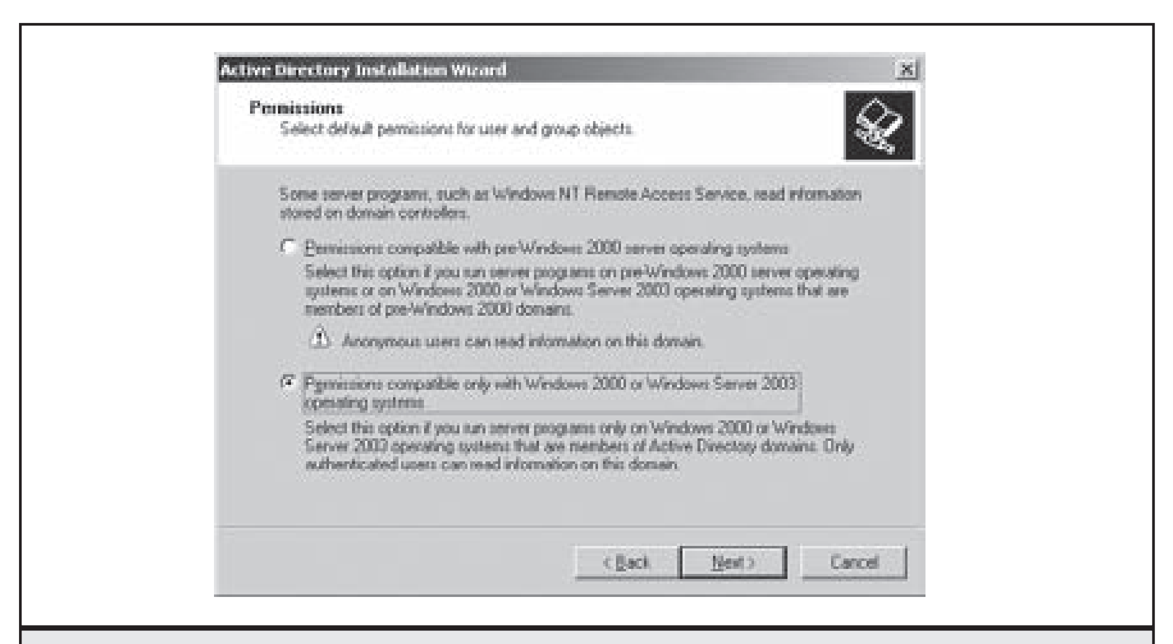


Figura 21-10. Seleccionar el estilo del permiso a utilizar para el dominio nuevo.

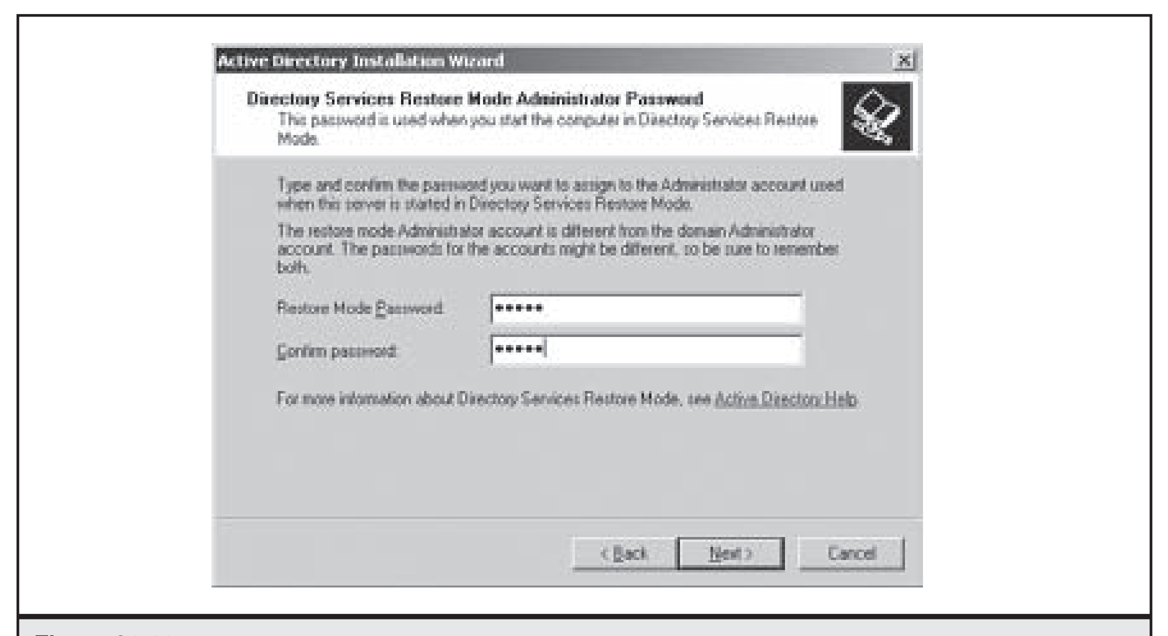


Figura 21-11. Asignar una contraseña de administrador en el modo de recuperación.

Una vez que se ha configurado el domino y el sistema se ha reiniciado, usted podrá administrarlo por medio de las nuevas herramientas que aparecerán en el fólder Administrative Tools del menú Start. Las herramientas más importantes son:

- Active Directory Users and Computers
- Active Directory Sites and Services
- Active Directory Domains and Trusts

Si está aprendiendo Windows Server 2003, debe invertir algún tiempo explorando estas herramientas, en particular las del programa Active Directory Users and Computers, el cual se utiliza regularmente para administrar cuentas de usuario y de computadoras en las redes de producción.

AGREGAR LAS TAREAS DHCP Y WINS

Las otras dos tareas que son importantes en la mayoría de las redes son Dynamic Host Configuration Protocol (DHCP), la cual asigna automáticamente las direcciones IP a los clientes de la red y Windows Internet Naming Service (servicio WINS), que compara los antiguos nombres NetBIOS con direcciones IP en la red.

Para agregar la tarea DHCP, comience en la ventana Configure Your Server, seleccione DHCP Server y haga clic en Next. Lo anterior instala el servicio DHCP y, después, inicia un proceso para definir el alcance del nuevo rango del DHCP.

Los servidores DHCP administran el rango de direcciones IP que asigne y las distribuyen en las computadoras cliente y en otros dispositivos (como las impresoras de red) que están configuradas para obtener su dirección IP de un servidor DHCP. Solo un servidor DHCP puede estar activo en una red a la vez. Cuando una computadora cliente se inicia, envía una solicitud para que el servidor DHCP le asigne una dirección. El servidor DHCP de la red “escucha” la solicitud y le asigna una dirección al dispositivo de entre su rango de direcciones disponibles (el alcance). En la figura 21-12 se muestra el comienzo del New Scope Wizard.

Después de hacer clic en Next para continuar, observará la figura 21-13, en la que puede asignar un nombre al nuevo alcance, que sea descriptivo. En algunos casos, querrá configurar múltiples alcances, siempre y cuando no se encimen. Por ejemplo, usted podría querer un alcance diferente para las impresoras, los clientes o las diferentes partes de la compañía. Sin embargo, en redes pequeñas, un solo alcance es más que suficiente. Luego de ingresar un nombre y una descripción, presione Next para continuar.

Ahora defina el rango del alcance y la máscara de subred que deberá asignarse. En el ejemplo que se muestra en la figura 21-14, el servidor DHCP manejará el rango de direcciones desde la 192.168.1.150 hasta la 192.168.1.255 y utilizará una máscara de subred de 8 bits, la cual corresponde a 255.0.0.0. Para su red, ingrese los valores apropiados y haga click en Next para continuar.



Figura 21-12. El New Scope Wizard para configurar el alcance DHCP.



Figura 21-13. Seleccionar un nombre y una descripción para el nuevo alcance DHCP.

Figura 21-14. Asignar el rango de direcciones del alcance y la máscara de la subred.

Ahora se le da la opción de excluir cualquiera de las direcciones dentro del rango de alcance, lo que se muestra en la figura 21-15. En esencia, ésta "separa" parte del rango del alcance DHCP. Si usted no tiene direcciones que excluir, simplemente presione Next para continuar.

Ahora puede seleccionar la duración a utilizar en las rentas de direcciones DHCP. Una renta es un periodo durante el cual una computadora en particular puede tener la misma dirección IP asignada para el servidor DHCP. En la mayoría de las situaciones, es apropiada la duración de la renta por omisión de ocho días. En particular, una duración más corta puede ser necesaria en redes muy apretadas que no cuentan con muchas direcciones disponibles, de forma que sea más probable que el servidor cuente con una dirección disponible para dispositivos que se conectan solo de forma periódica. La figura 21-16 muestra la pantalla Lease Duration dentro del New Scope Wizard.

A continuación, tiene la oportunidad de configurar direcciones adicionales que también se proporcionan a computadoras cliente cuando éstas obtienen su dirección IP. Los servidores DHCP pueden también asignar la dirección del servidor DNS, la dirección de acceso y la dirección WINS, mientras que asignan la dirección IP y la computadora cliente entonces utiliza estos otros parámetros automáticamente. Cuando usted selecciona Yes, I Want to Configure These Options Now y teclea Next, se le van a presentar varias pantallas en las que puede definir, a la vez:

- La compuerta por omisión
- El nombre de dominio y las direcciones del servidor DNS
- La dirección del servidor WINS

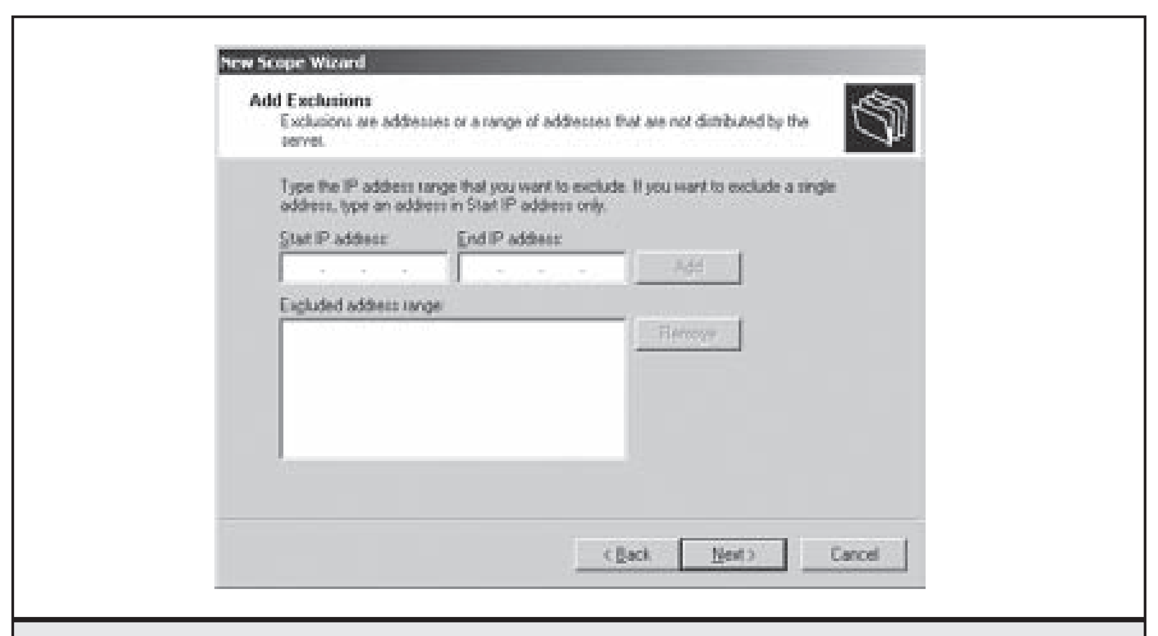


Figura 21-15. Excluir direcciones del alcance DHCP.

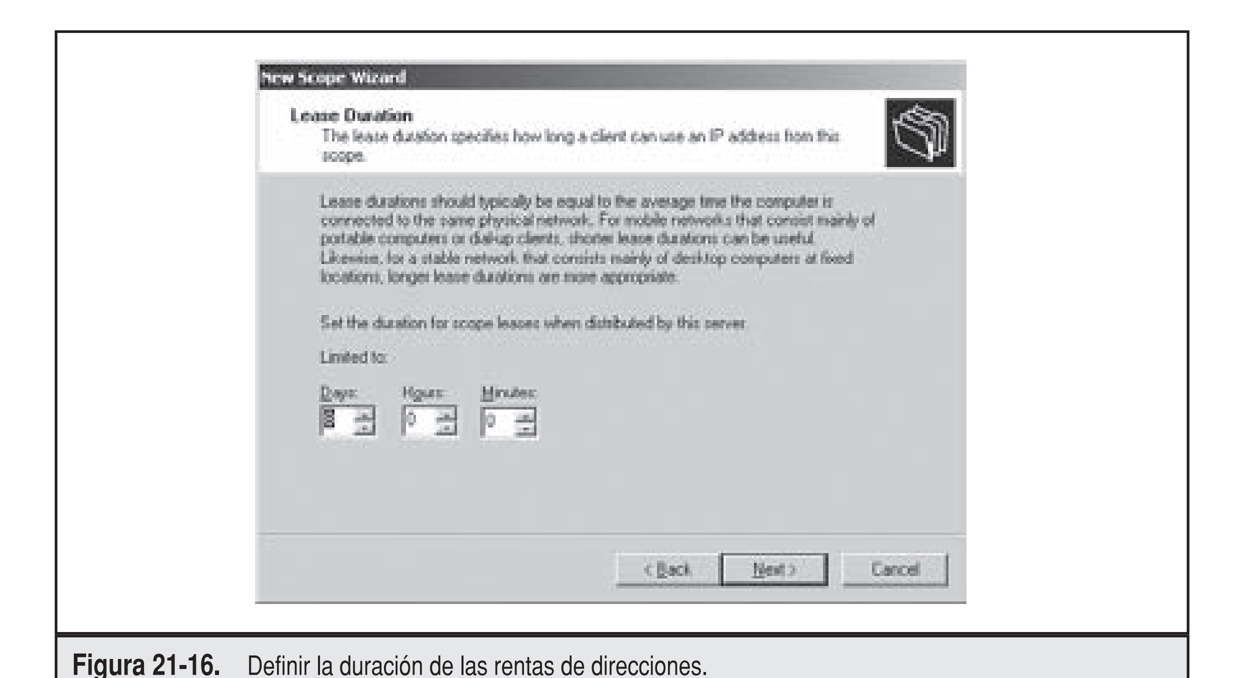


Figura 21-16. Definir la duración de las rentas de direcciones.

Después de terminar la instalación de la tarea del DHCP, usted también deberá agregar la tarea del WINS, suponiendo que ésta no se encuentra corriendo ya en la red. La tarea del WINS agrega un servicio WINS al servidor. El aspecto atractivo respecto a agregar la tarea, es que su instalación no necesita ninguna configuración en particular. Los servidores WINS corren automáticamente y detectan los nombres y direcciones del NetBIOS que utilizan las computadoras conectadas a ellos. Todo lo que debe hacerse para usar un servidor WINS es instalarlo, y después hacer que las diferentes computadoras de la red utilicen la dirección del servidor como un WINS.

AGREGAR TAREAS DE SERVIDOR DE ARCHIVO Y SERVIDOR DE IMPRESIÓN

Probablemente, las dos tareas más comunes de un servidor son las de archivo y la de impresión. El primero almacena los archivos en los que los usuarios tienen acceso a través de la red. Los archivos almacenados se guardan utilizando la seguridad del servidor de archivos, además de que se encuentran convenientemente localizados para respaldarse en cinta o en cualquier otro medio. El segundo, acepta trabajos de impresión de las computadoras cliente y los envía a la impresora apropiada conectada a la red.

Del Configure Your Server Wizard, seleccione File Server y haga clic en el botón Next. La primera pantalla que aparece le permite habilitar las cuotas del disco para los usuarios (vea la figura 21-17), éstas le ayudan a establecer límites de espacio en disco que puede administrar en forma

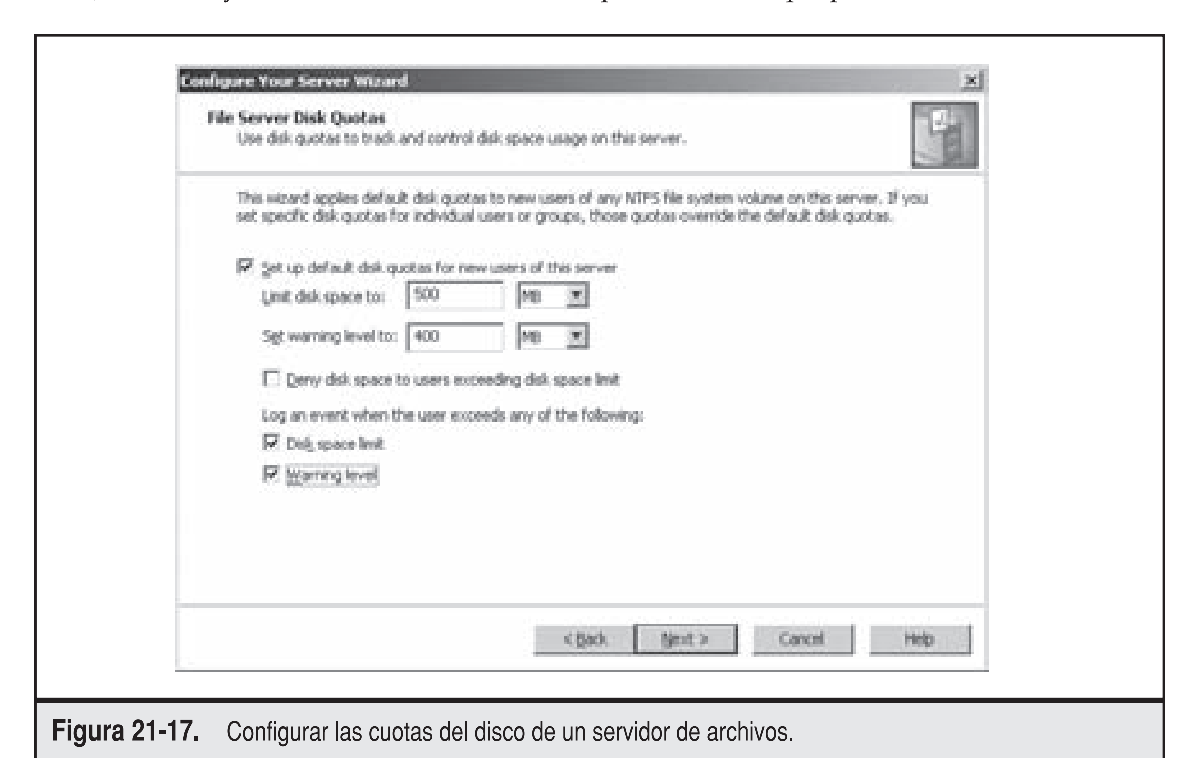


Figura 21-17. Configurar las cuotas del disco de un servidor de archivos.

fácil a los usuarios de la red. Puesto que los servidores no cuentan con una cantidad ilimitada de espacio en disco y que un usuario que utilice una gran cantidad de espacio podría saturar el servidor afectando a todos los demás usuarios, tiene sentido utilizar las cuotas en el disco. Complete la caja de diálogo como lo considere apropiado y haga click en Next para continuar.

A continuación se le solicita instalar el Indexing Service en el servidor. Este servicio a menudo indexa el contenido de todos los archivos almacenados en el servidor, lo cual permite que su búsqueda sea muy rápida. Sin embargo, el proceso de indexado consume recursos del servidor, por lo que solo debe habilitarlo cuando crea que el beneficio de encontrar el índice rápidamente justifica el costo de mantener el índice actualizado. Para un servidor con un procesador rápido y poca actividad del usuario, puede habilitar esta facilidad sin tener que preocuparse por el costo. Presione Next para continuar.

Después, podrá observar una pantalla de resumen con las opciones que hizo. Si son correctas, haga clic en Next para terminar la instalación de la tarea File Server. Una vez terminada, podrá ver el asistente Share a Folder, el cual le permite instalar sus primeros fólders compartidos. Puede crear uno utilizando el asistente; de otra forma Configure Your Server Wizard no mostrará la tarea File Sharing como instalada.

Cuando selecciona agregar la tarea Print Server al servidor en el Configure Your Server Wizard, se le solicita solamente el nivel de soporte que el servidor de impresión debe brindar. Puede seleccionar entre soportar solo a clientes Windows 2000 y Windows XP, o a todos los clientes de Windows. Si todas sus computadoras cliente corren al menos Windows 2000, entonces puede seleccionar sin ningún problema el soporte más limitado; de otra forma seleccione All Windows Clients en la pantalla de la figura 21-18.

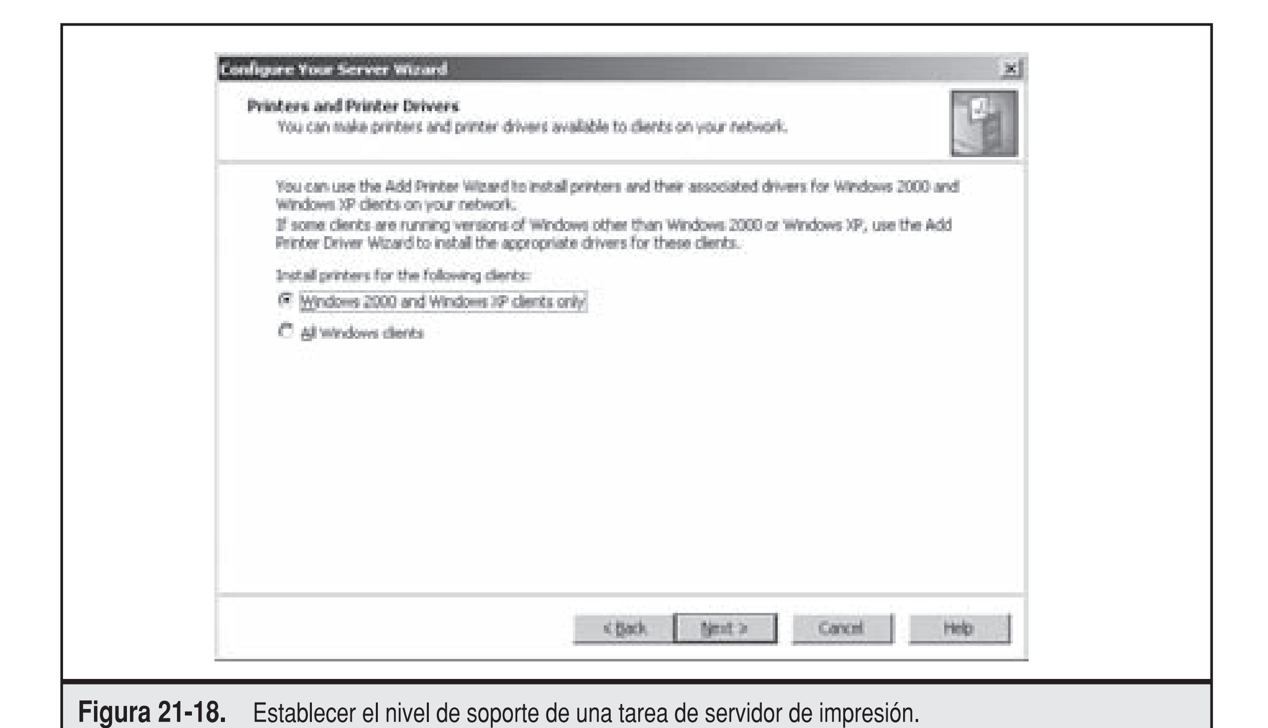


Figura 21-18. Establecer el nivel de soporte de una tarea de servidor de impresión.

La instalación de la tarea del servidor de impresión inicia un asistente en forma automática, en el cual puede seleccionar instalar una impresora compartida inmediatamente. De otra forma, puede agregar impresoras al servidor de impresión utilizando el programa Add Printer en el fólder Printers and Faxes.

AGREGAR LA ADMINISTRACIÓN BASADA EN LA WEB

Windows Server 2003 puede administrarse en gran medida mediante una interfase web desde una computadora remota. Esta característica es parte de la tarea Application Server y también requiere un par de pasos de instalación adicionales.

Primero, utilice Configure Your Server Wizard para agregar la tarea Application Server, la cual instala los Internet Information Services y cualquier otro software adicional. Cuando se agrega la tarea Application Server Role, aparece la pantalla que se muestra en la figura 21-19, donde se le ofrece la opción de agregar también soporte para FrontPage Server Extensions y ASP.NET. Generalmente, recomiendo agregar ambos a menos que esté seguro de que no los va a necesitar.

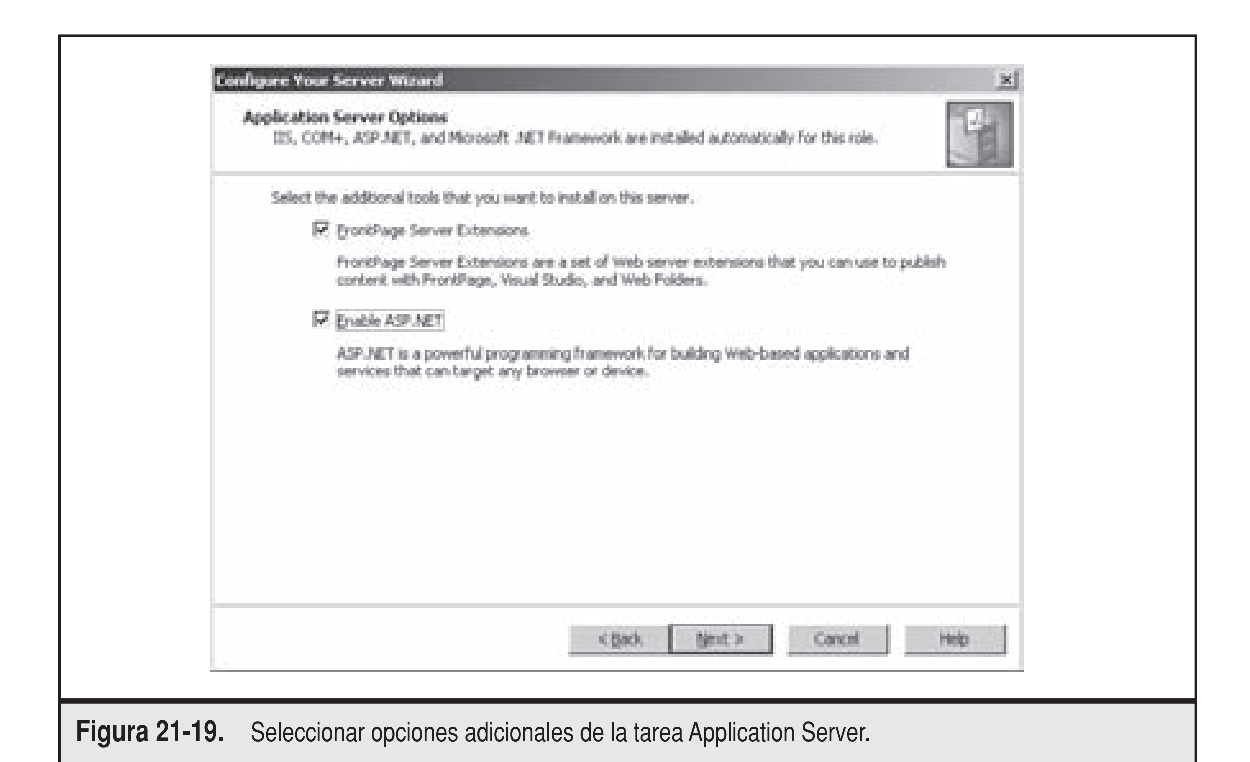


Figura 21-19. Seleccionar opciones adicionales de la tarea Application Server.

A continuación, debe instalar otro componente para habilitar la administración remota basada en la web, siguiendo los pasos siguientes:

1. Abra el Control Panel y seleccione Add/Remove Programs.
2. Haga clic en Add/Remove Windows Components del lado izquierdo de la ventana.
3. Seleccione Application Server y oprima el botón Details.
4. Haga clic en Internet Information Services (IIS) y en el botón Details.
5. Seleccione World Wide Web Service y oprima el botón Details.
6. Haga clic en Remote Administration (HTML) (vea la figura 21-20), después haga clic en el botón OK en cada ventana que se abra hasta que regrese al Windows Components Wizard, y después haga clic en Next para instalar el componente.

Después de instalar el componente de administración remota, podrá entrar a él utilizando el Internet Explorer. Para probarlo en la computadora local, abra el Internet Explorer y teclee la dirección siguiente:

```
https://localhost:8098
```

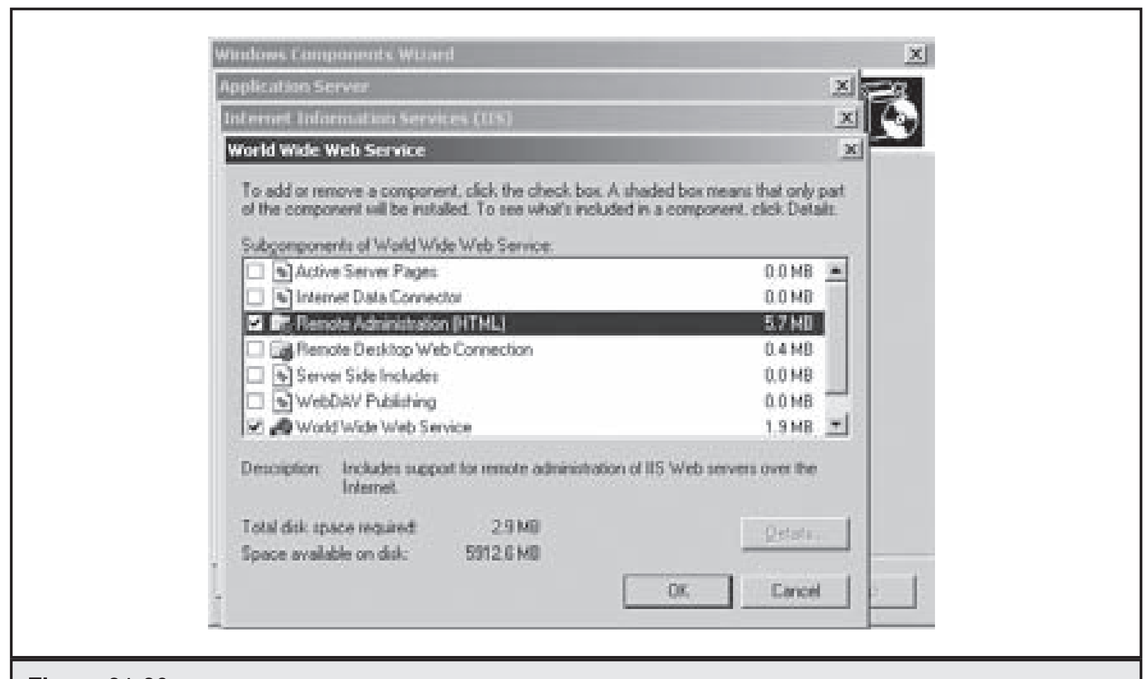


Figura 21-20. Agregar la facilidad Remote Administration (HTML).

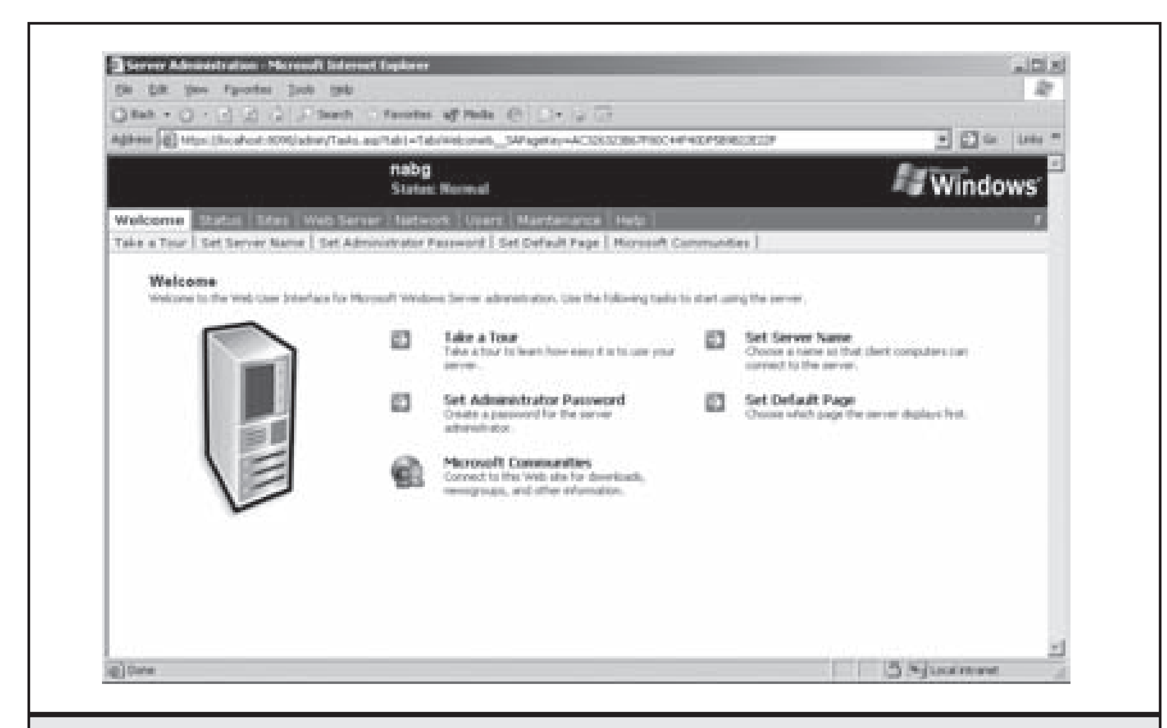


Figura 21-21. La página de inicio de la consola remota de administración del web.

Después verá una caja de diálogo solicitándole que confirme el certificado SSL, la página de inicio del sitio de administración se deberá abrir, como se muestra en la figura 21-21. Para entrar al sitio desde otra computadora, usted puede utilizar una de los formatos de dirección siguientes, sustituyendo *xxx.xxx.xxx.xxx* por la dirección IP del servidor, o por *server_name* con el nombre del servidor NetBIOS del servidor:

```
https://xxx.xxx.xxx.xxx:8098
https://server_name:8098
```

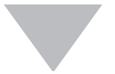
RESUMEN DEL CAPÍTULO

Como ha visto en este capítulo, la configuración de Windows Server 2003 es más fácil que hacer una configuración similar en versiones. El asistente Configure Your Server le permite agregar fácilmente tareas a un servidor. Además, el programa Manage Your Server le proporciona un lugar centralizado en el cual podrá administrar y agregar o quitar un servidor. Una vez que se agrega una tarea, se puede tener acceso a todos los programas de administración tradicionales a fin de administrar esos servicios.

CAPÍTULO 22

Instalación de Linux con una configuración de servidor

Un componente clave del éxito de Linux ha sido la mejora significativa en las herramientas de instalación. Lo que alguna vez fue un proceso un poco aterrador, se ha convertido ahora en algo casi trivial. La mejora en las diferentes maneras en las que usted puede instalar el software ha sido aún mejor; aunque los CD-ROM sean la opción más común todavía, no son la única. Las instalaciones por medio de una red son parte de la lista de opciones por omisión y pueden ser muy convenientes cuando se va a instalar un gran número de hosts.



PISTA En el lenguaje de UNIX (o Linux), un host es cualquier computadora en una red, sin considerar si está trabajando como un servidor de algún tipo o como estación de trabajo.

La mayoría de las configuraciones por omisión en las que puede instalarse Linux ya son capaces de crear un servidor. Desafortunadamente, esto es debido a una decisión de diseño ligeramente ingenua: un servidor proporciona servicios a todos —desde servicios de disco hasta impresoras, correo, noticias, casi a todo—. A menudo, estos servicios se encuentran activos desde el principio, dependiendo de la distribución que utilice y si se instaló como estación de trabajo o servidor. Como usted sabe, la realidad de la mayoría de los servidores es que están exclusivamente dedicados a llevar a cabo una o dos tareas y cualquier otro servicio instalado simplemente consume espacio en la memoria y reduce el desempeño.

Este capítulo analiza el proceso de instalación de Red Hat Enterprise Linux ES en la medida que tiene que ver con los servidores. Este proceso requiere dos cosas: establecer la diferencia entre servidores y estaciones de trabajo del cliente y acelerar la operación de un servidor con base en su propósito.



PISTA Con una variedad de distribuciones Linux disponibles, ¿por qué este análisis se enfoca en Red Hat? La respuesta es simple: Red Hat es popular y técnicamente atractivo. Es muy amigable para muchos tipos de usuarios y usos y, si usted tiene que instalarlo por primera vez, también es amigable al usuario. (¡Que toda la distribución esté disponible gratis en Internet es solo una ventaja más!). Conforme se vuelva experto en Linux, podrá encontrar otras distribuciones interesantes y analizarlas. Después de todo, es una de las ventajas de los usuarios de Linux dondequiera que la libertad de elección sea algo crucial. Usted no deber sentirse atrapado con un sistema propietario.

CONFIGURAR EL HARDWARE DE LA COMPUTADORA PARA LINUX

Antes de que usted inicie la fase de instalación en sí, evalúe dos cosas importantes:

- ¿Con qué hardware correrá el sistema?
- ¿Cómo deberá configurar el servidor para ofrecer los servicios que necesita de él?

Comencemos examinando los problemas relativos al hardware.

Hardware

Como en cualquier sistema operativo, es prudente determinar qué configuraciones de hardware pueden funcionar antes de comenzar un proceso de instalación. Cada proveedor comercial publica una lista de compatibilidad de hardware (HCL) que está disponible en su sitio web. Asegúrese de adquirir las versiones más actuales de ellas, a fin de que esté seguro de que el proveedor proporcionará soporte a todo el hardware que va a utilizar. En general, la mayoría de las configuraciones más populares que se basan en Intel funcionan sin ninguna dificultad. La página web de la lista de compatibilidad de hardware de Red Hat se encuentra en **http://bugzilla.redhat.com/hwcert**, y para el Linux SUSE de Novell, puede encontrarla en **http://developer.novell.com/yessearch/Search.jsp**.

Una sugerencia general que se aplica a todos los sistemas operativos es evitar configuraciones de hardware y software muy arriesgadas. Aunque éstas parezcan muy impresionantes, no han experimentado el proceso de maduración que parte del hardware ligeramente más antiguo ha sufrido. Para los servidores, la tentación de utilizar una configuración muy arriesgada generalmente no representa un problema ya que no necesitan contar con la última y más sofisticada tecnología, como tarjetas de video muy llamativas. Después de todo, el objetivo principal es ofrecer un servidor con una disponibilidad muy alta para los usuarios de la red y no jugar Doom 3.

Diseño del servidor

Cuando un sistema se convierte en un servidor, su estabilidad, disponibilidad y desempeño representan temas esenciales. Estos tres problemas generalmente se resuelven al comprar más hardware, lo cual es desafortunado. Pagar miles de dólares adicionales para obtener un sistema capaz de alcanzar los tres objetivos, cuando el nivel de desempeño deseado pudo haberse alcanzado al darle mantenimiento al hardware existente, es una molestia que se debe evitar. Con Linux, lograr estos objetivos sin gastar demasiado dinero no es difícil. ¡Aún mejor, las ganancias son enormes!

La decisión de diseño más importante que debe tomar cuando administre una configuración de servidor no es técnica, sino administrativa. Debe diseñar un servidor que no sea amigable con los usuarios casuales, lo cual significa no instalar herramientas multimedia sofisticadas, no brindar soporte a tarjetas de sonido y no instalar navegadores web muy estilizados (cuando sea posible). De hecho, su organización deberá establecer una regla en la que se establezca la estricta prohibición de usar de manera informal el servidor. Esta regla deberá aplicarse no solamente a los usuarios del sitio, sino también a los administradores.

Otro aspecto importante del diseño de un servidor es asegurarse de que cuenta con un ambiente agradable. Como administrador de sistemas, deberá asegurar el bienestar físico de sus servidores, manteniéndolos en un cuarto independiente y físicamente seguro. El único acceso a los servidores que tendrá el personal no administrativo deberá ser a través de la red. El cuarto del servidor en sí deberá estar bien ventilado, frío y cerrado. El no asegurarse de que existan estas condiciones ambientales significa que se deberá esperar un accidente. Los sistemas que se sobrecalientan y los usuarios que "creen" que saben cómo resolver todos los problemas, representan tanto peligro (sin lugar a dudas, aún un mayor peligro) para la estabilidad del servidor que un software defectuoso. Además, Linux es particularmente vulnerable a los intrusos en la línea de comandos.

Una vez que el sistema está bien seguro detrás de puertas cerradas, la instalación de las baterías de respaldo es también crucial. Este respaldo sirve para dos propósitos principales: mantener el sistema operando durante una falla de alimentación de forma que se apague paulatinamente y, por tanto, se evite la pérdida de cualquier archivo. El otro es asegurarse de que los picos y las caídas de voltaje, así como los diferentes ruidos eléctricos no interfieran con la salud de su sistema.

Para mejorar la situación de su servidor, puede tomar las acciones específicas siguientes:

- Aproveche el hecho de que la GUI no está acoplada al sistema operativo principal y evite comenzar X Windows a menos que alguien necesite sentarse en la consola y correr una aplicación. Después de todo, X Windows, como cualquier otra aplicación, requiere de memoria y tiempo de trabajo del CPU, los cuales será mejor que sean utilizados en los procesos del servidor.
- Determine qué funciones quiere que lleve a cabo el servidor y deshabilite todas las demás. Las funciones que no se utilizan no solo representan un desperdicio de memoria y tiempo del CPU, sino que también implican otro problema de seguridad que necesitará resolver.
- Linux, a diferencia de otros sistemas operativos, le permite seleccionar las características que desea que tenga el kernel. El kernel por omisión con el que cuenta está razonablemente bien sintonizado, por lo que no necesitará ajustarlo. Sin embargo, si necesita modificar una característica o mejorar un kernel, sea selectivo en cuanto a lo que agrega y lo que conserva. Asegúrese de que necesita una determinada facilidad antes de instalarla.

Tiempo de operación

Toda esta discusión acerca del cuidado que se debe tener con los servidores y de la importancia de asegurarse de que las adiciones no provoquen que dejen de funcionar, proviene de una vieja filosofía de UNIX: *El tiempo de operación es bueno. Más tiempo de operación es mejor*.

El comando **uptime** le dice al usuario cuánto tiempo ha estado el sistema en operación desde su último reinicio, cuántos usuarios se encuentran en ese momento conectados y cuánta carga está soportando. Las dos últimas estadísticas son mediciones útiles necesarias para conservar la salud diaria del sistema y la planeación a largo plazo. Por ejemplo, si la carga en el servidor se ha conservado elevada de manera consistente, debe considerar la adquisición de un servidor con mayor capacidad.

Sin embargo, el número más importante es cuánto tiempo ha estado el servidor operando desde su último reinicio. Los tiempos de operación prolongados son signo de un adecuado cuidado, mantenimiento y, desde un punto de vista práctico, de una estabilidad del sistema. A menudo encontrará administradores de UNIX que presumen acerca de los elevados tiempos de operación de sus servidores de la misma manera que escuchará a los aficionados de autos elogiar la potencia de los caballos de fuerza. Este enfoque en el tiempo de operación es también la razón por la que escucha a los administradores de UNIX hacer comentarios precipitados respecto a instalaciones de Windows que requieren una reinicialización por cada cambio pequeño. En contraste, se verá fuertemente presionado por encontrar cualquier modificación al sistema UNIX que requiera ser reiniciado a fin de que el cambio se lleve a cabo.

Problemas en el doble arranque

Si usted es principiante en Linux, de seguro no estará listo para comprometer el uso de un sistema completo con el propósito de "ponerlo a prueba". Debido a que la gente que diseñó Linux comprende que vivimos en un mundo heterogéneo, todas las distribuciones de Linux han sido diseñadas de forma que puedan instalarse en particiones independientes de su disco duro, mientras que las restantes se pueden dejar vacías. En general, lo anterior significa que Microsoft Windows puede coexistir en una computadora que pueda también correr Linux.

Debido a que el enfoque de este capítulo es la instalación del servidor, esta sección no abordará los detalles de la construcción de un sistema de doble arranque. No obstante, cualquier persona con un poco de experiencia en la creación de particiones de un disco, deberá ser capaz de imaginarse cómo construir dicho sistema. Si encuentra dificultades, podrá referirse a la guía de instalación que vino con su distribución o a cualquier otra de tantas guías para principiantes de Linux que se encuentran disponibles en el mercado.

Para volver a particionar un sistema al que ya se le ha instalado Windows 9x, NT, 2000 o XP, sin volver a formatear el disco y reconstruir todo desde el principio, puede utilizar un programa de software disponible en el mercado, como PartitionMagic.

Métodos de instalación

Con la conectividad y las velocidades mejoradas de las redes de área local y las conexiones de Internet, una opción cada vez más popular es llevar a cabo las instalaciones a través de la red, en lugar de utilizar un CD-ROM local.

En general, encontrará que la instalación de las redes cobra importancia una vez que decide utilizar Linux en muchas máquinas y que requiere un procedimiento rápido de instalación donde muchos sistemas puedan instalarse en paralelo.

Típicamente, la instalación de servidores no es muy apropiada para que sea automática, ya que cada servidor generalmente tiene una tarea específica y, por tanto, una configuración un poco diferente. Por ejemplo, un servidor dedicado al manejo de información de acceso que se le envía a través de la red, tendrá configuradas particiones especialmente grandes para los directorios de acceso en comparación con un servidor de archivos que no lleve a cabo el acceso a la red por sí mismo.

Debido a que los servidores generalmente no se instalan utilizando una filosofía "un sol tamaño sirve para todo", el enfoque en esta sección es exclusivamente en la técnica utilizada para la instalación de un sistema a partir de CD-ROM. Desde luego que después de que usted haya seguido paso a paso el proceso de instalación, encontrará que llevarlo a cabo por medio de la red será un proceso muy directo.

Si no llegara a funcionar bien…

Ha llevado a cabo el proceso de instalación… dos veces. Este libro afirmaba que debía funcionar. El manual de instalación decía que debía funcionar. El gurú de Linux con el que hablé la semana pasada dijo que debía funcionar.

Sin embargo, no funciona.

En palabras inmortales de Douglas Adams: "No se asuste". Ningún sistema operativo se instala sin problemas 100 por ciento de las veces. (¡Sí, ni siquiera el Mac OS!). El hardware no siempre trabaja como se anuncia, las combinaciones del hardware entran en conflicto unas con otras, o ese CD-ROM que le grabó un amigo tiene errores de CRC. (Recuerde: ¡Es totalmente

lícito que su amigo haga una copia de Linux!). O, el software tiene un error, aunque usted haya deseado que no lo tuviera.

Con Linux, usted cuenta con algunas opciones que puede llevar a cabo para conseguir ayuda. Si ha comprado una copia de Caldera o Red Hat, puede contactar al departamento de soporte técnico del distribuidor y hablar con alguna persona experta que pueda resolver el problema con usted. Si no compró el software en caja, puede tratar de contactar compañías como Levanta (**http://www.levanta.com**), la cual es una compañía comercial dedicada a proporcionar ayuda. Por último, pero seguramente no menos importante, es la opción de contactar otras fuentes de ayuda en línea. Existen miriadas de sitios disponibles en la web para ayudarle a comenzar el trabajo, los que no solo contienen consejos y trucos útiles, sino que también proporcionan documentación y foros de análisis donde puede proponer sus preguntas. Obviamente, deseará comenzar con el sitio dedicado a su distribución **—http://www.redhat.com** para Linux Red Hat y **http://www.novell.com** para Linux SUSE. (Otras distribuciones tienen sus propios sitios en la red. Visite a su distribuidor para obtener información).

A continuación se listan algunas fuentes en línea recomendadas para obtener ayuda relacionada con la instalación:

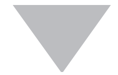
▼ **comp.os.linux.domain** Es un grupo de noticias, no un sitio en la web. Puede leerlo en **http://groups-beta.google.com**.

▲ **http://tldp.org** Este sitio (el nombre es una abreviatura de The Linux Documentation Project) es una colección de información muy importante respecto a todo tipo de temas relacionados con Linux, incluyendo guías de instalación. No obstante, va una advertencia: no todos los documentos están actualizados. Asegúrese de verificar cuándo fue la última vez que se actualizó el documento antes de seguir las instrucciones. Existe también una mezcla de guías de ayuda tipo receta de cocina, así como también guías que proporcionan explicaciones más completas de qué está pasando.

INSTALACIÓN DE LINUX RED HAT

Esta sección documenta los pasos necesarios para instalar Red Hat Enterprise Linux ES en un sistema independiente, por medio de un método liberal del proceso, que orienta sobre la instalación de todas las posibles herramientas relevantes a las operaciones del servidor. En capítulos posteriores se explica el propósito de cada subsistema y lo orienta a determinar si es necesario que lo conserve.

Usted cuenta con dos formas de iniciar el proceso de arranque: puede utilizar un disco flexible de arranque o un CD-ROM. Esta guía de instalación supone que usted arrancará del CD-ROM para comenzar el procedimiento de instalación de Red Hat. Si cuenta con una máquina anterior en la que no se pueda arrancar desde el CD-ROM, necesitará utilizar un disco de arranque y comenzar el procedimiento desde ahí.



PISTA El utilizar el disco de arranque altera el orden de algunos pasos durante la instalación, como qué lenguaje escoger y si debe usar un disco duro o un CD-ROM. Una vez que haya superado las diferencias iniciales, podrá observar que los pasos gráficos son los mismos.

Si su sistema soporta CD-ROM que se puedan arrancar, éstos proporcionan un método más rápido. Si su distribución no vino con un disco de arranque y no puede arrancar desde el

CD-ROM, necesita crear un disco de arranque. Este análisis supone que cuenta con una instalación de Windows funcionando para crearlo.



PISTA ¿Qué pasa si no desea utilizar un instalador gráfico? No se preocupe. Red Hat está consciente de que mucha gente aún prefiere las herramientas de instalación basadas en texto y que algunas personas necesitan utilizar estas herramientas en sistemas que no soporten gráficos. Si se encuentra en alguna de estas categorías, teclee text en el boot: cuando arranque Linux ya sea desde el CD-ROM o desde el disco flexible.

Crear un disco de arranque

Una vez que se ha iniciado Windows y el CD-ROM se encuentra en el drive apropiado, abra la ventana MS-DOS Command Prompt (haga click en Start y seleccione Programs | Command Prompt), la cual le da una ventana de símbolo del sistema. Cámbiese al drive donde se localiza el CD-ROM y vaya al directorio **dosutils**. Ahí encontrará el programa **rawrite.exe**. Simplemente corra el programa ejecutable, que le preguntará por el archivo fuente y el disco flexible de destino.

El archivo fuente se encuentra en el mismo drive y se llama **.img**.

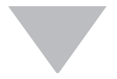
Comenzar la instalación

Para comenzar el proceso de instalación, arranque el CD-ROM, lo que le desplegará una pantalla que le presentará a Red Hat Enterprise Linux ES. En el fondo de la pantalla aparecerá el comando siguiente:

```
boot:
```

Si no presiona ninguna tecla, el mensaje automáticamente comienza el proceso de instalación. Usted puede presionar la tecla ENTER para iniciar el proceso de inmediato.

Si ya ha tenido alguna experiencia con instalaciones de Red Hat en el pasado y no desea que el sistema realice pruebas en su hardware de forma automática, puede teclear **expert** cuando aparezca el boot: en la mayoría de las instalaciones, sin embargo, usted querrá utilizar el procedimiento por omisión. (En Linux, la instalación de experto en realidad significa *experto*, por lo que no deberá utilizarla si no cuenta con el conocimiento y la experiencia suficientes en Linux).



NOTA Como parte inicial de las cargas del sistema operativo y de las detecciones automáticas del hardware, no se sorprenda si no detecta el subsistema SCSI. El soporte de SCSI se activa posteriormente durante el proceso.

Seleccionar el idioma

El programa primero despliega un menú que le pregunta qué idioma desea utilizar para continuar con el proceso de instalación (vea la figura 22-1).

La interfase trabaja de manera muy similar a cualquier otra del tipo Windows. Simplemente márquela y haga clic en su selección. Cuando esté listo, presione el botón Next en la parte inferior derecha de la pantalla.

En el lado izquierdo de la pantalla se encuentra la ayuda sensible al contexto. Si no desea verla, puede hacer clic en el botón Hide Help en la parte inferior izquierda de la pantalla.

El botón Back en la parte inferior derecha se encuentra en color gris en este punto ya que no ha habido anteriormente opciones que seleccionar.

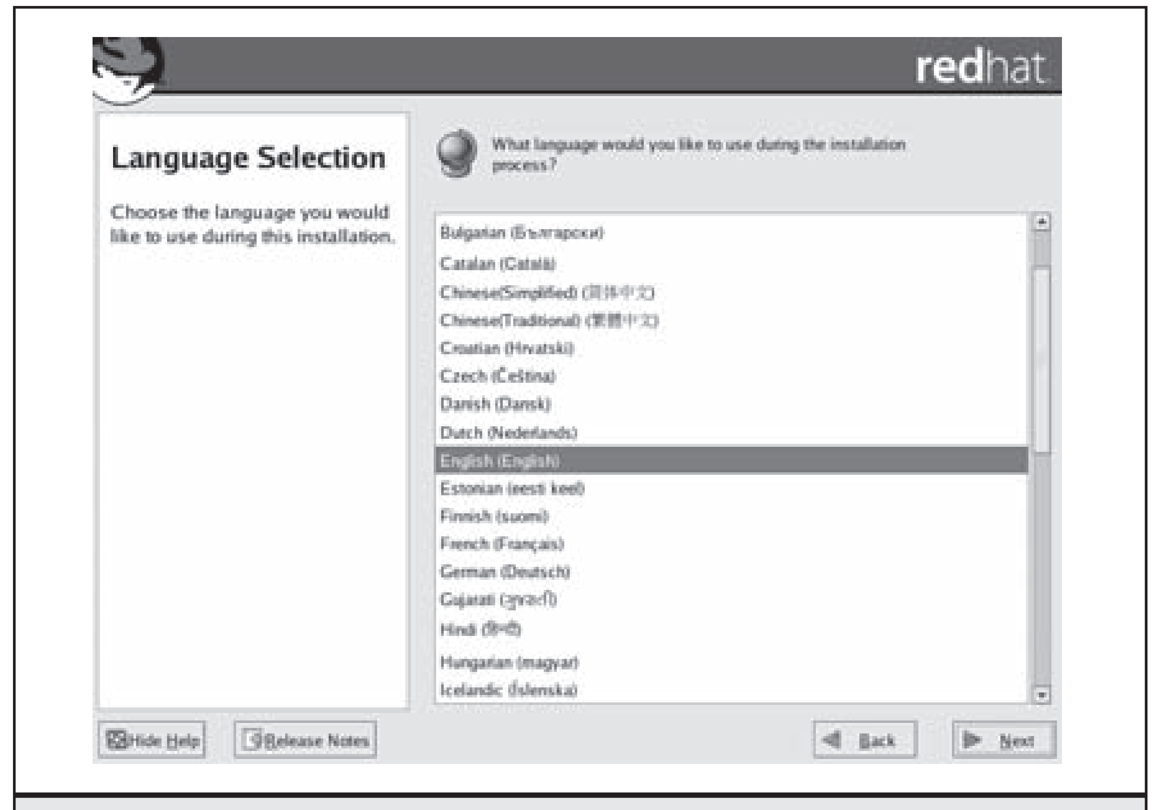


Figura 22-1. Seleccionar un idioma durante el proceso de instalación.

Seleccionar el tipo de teclado

El siguiente menú le permite seleccionar el tipo de teclado que tiene. Las opciones se encuentran divididas en tres cajas de diálogo: la primera lista los tipos de teclados soportados; la segunda, las diferentes distribuciones que el teclado puede tener; y la tercera, le permite seleccionar variantes adicionales que se encuentran disponibles. La caja de diálogo que se encuentra en la parte más inferior sirve para que teclee para que pueda hacer pruebas para ver si su teclado está funcionando correctamente; aunque no tiene que teclear nada en la caja de diálogo si no lo desea.

Para la mayoría de los administradores, el tipo de teclado será una de las opciones genéricas, la distribución del teclado será U.S. English (vea la figura 22-2), y en las variantes se seleccionará None.

Si alguna vez quisiera modificar el tipo o distribución de su teclado, puede utilizar el programa Keyboard que se encuentra en el menú Applications/Preferences.

Cuando termine, haga clic en Next para continuar o seleccione Back para regresar al menú de selección del idioma.

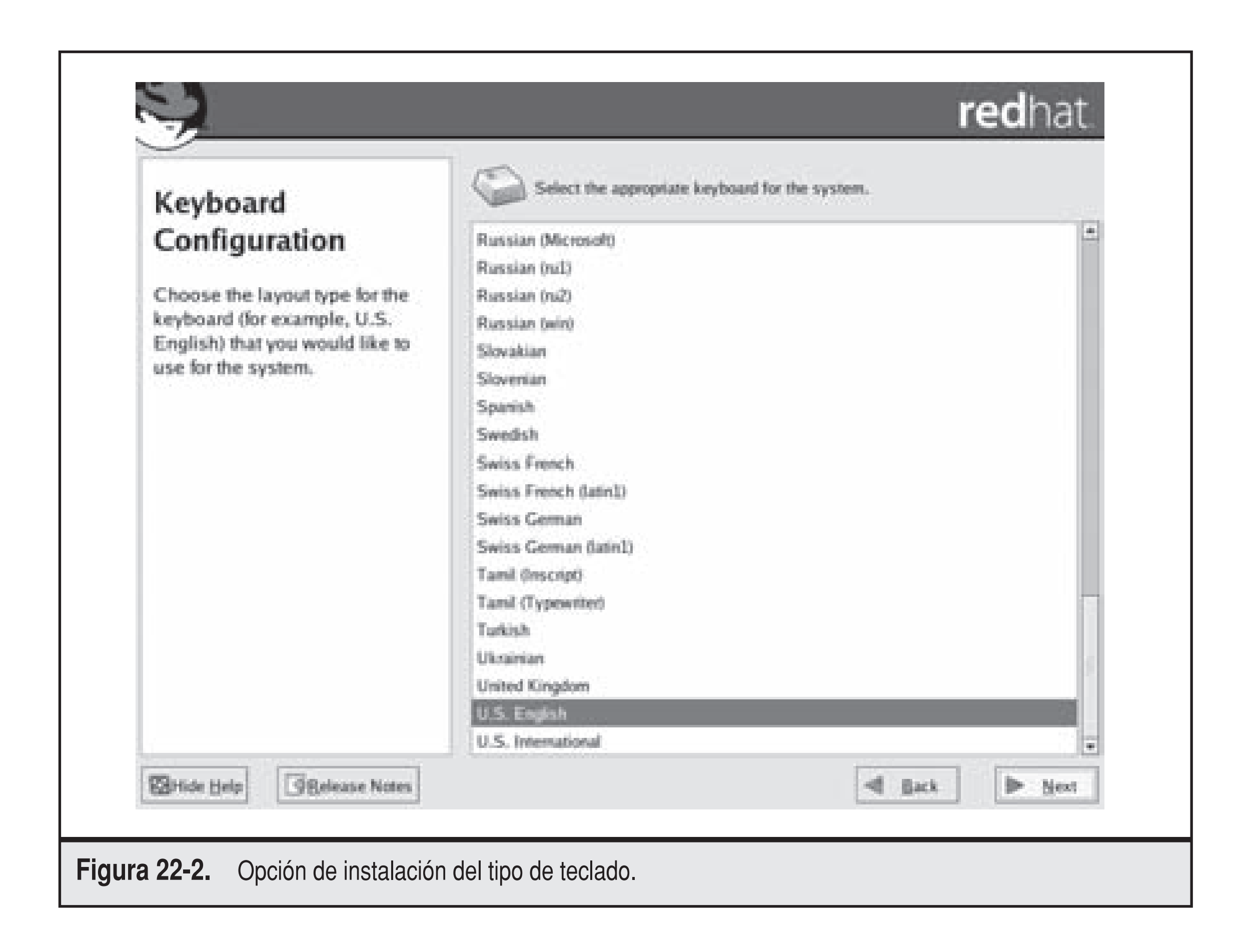


Figura 22-2. Opción de instalación del tipo de teclado.

Bienvenido a Linux Red Hat

Una vez que se han seleccionado los dispositivos de entrada y los idiomas, usted está ya listo para comenzar la fase de instalación de Red Hat Linux.

Crear particiones en Linux

A continuación seleccione cómo particionar su disco duro para Linux, lo cual es diferente a particionar discos en Windows. En pocas palabras, cada partición es *montada* en el tiempo de arranque. El proceso de montaje pone disponible el contenido de esa partición como si ésta fuera cualquier otro directorio en el sistema. Así, por ejemplo, el directorio raíz (/) se encuentra en la primera partición (*raíz*). En el directorio raíz se encuentra un subdirectorio llamado / usr, sin embargo está vacío. Usted puede entonces montar una partición independiente de forma que al ir al directorio / usr, le permita ver el contenido de la nueva partición montada (vea figura 22-3).

Debido a que todas las particiones, cuando se montan, parecen como un árbol unificado de directorios en vez de controladores separados, el software de instalación no diferencia entre una partición y la otra. Todo lo que le interesa es qué directorio deberá colocar en cada archivo. Como resultado, el proceso de instalación distribuye de manera automática sus archivos mediante

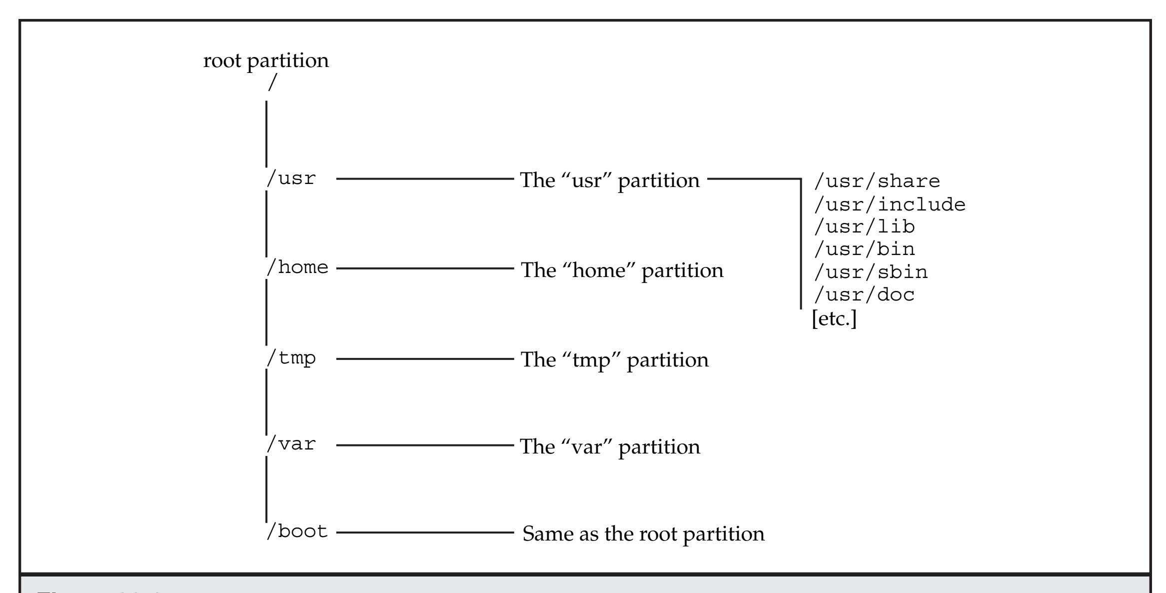


Figura 22-3. Qué tan separadas están las particiones en un solo árbol de directorios.

todas las particiones montadas, siempre y cuando éstas representen las diferentes partes del árbol de directorios donde los archivo generalmente se colocan. En Linux, el agrupamiento más significativo de archivos se presenta en el directorio / usr, donde residen todos los programas. (En términos de Windows, este directorio es similar a Program Files).

Debido a que está configurando un servidor, debe estar consciente del gran agrupamiento adicional de archivos que existirá a lo largo de la vida útil del mismo. Dichos agrupamientos son los siguientes:

- **/usr** Aquí es donde todos los archivos de programas residirán (este grupo es similar al C:\Program Files).
- **/home** Aquí se encontrarán los directorios raíz de todos (suponiendo que este servidor contendrá estos directorios). Este agrupamiento es útil para evitar que los usuarios consuman el disco entero y dejen sin espacio a otros componentes críticos, como los archivos de registro.
- **/tmp** Los archivos temporales se colocan aquí. Debido a que este directorio está diseñado para que cualquier usuario pueda escribir sobre él, usted necesitará asegurarse de que los usuarios no abusen de este privilegio y llenen todo el disco manteniéndolo en una partición independiente.
- **/var** Este es el destino final de los archivos de registro. Debido a que los servidores externos (por ejemplo, visitantes de un sitio web) pueden afectar los archivos de registro, particionar estos archivos es importante; asegura que nadie pueda llevar a cabo un ataque de negación del servicio (denial of service, DoS) generando tal cantidad de claves de acceso que sature el disco duro.

- **Swap** Este no es un sistema de archivos accesible al usuario, sin embargo, es donde se almacena el archivo de memoria virtual. Aunque Linux (y otras variantes de UNIX también) puede utilizar un archivo normal en disco para almacenar la memoria virtual en la forma como lo hace Windows, comprobará que mantener el almacenamiento swap en su propia partición mejora el desempeño.

Una buena idea es crear múltiples particiones en un disco para Linux, en lugar de una sola partición grande, lo cual estará acostumbrado a hacer con Microsoft Windows. A medida que se familiarice con los cómos y porqués de Linux, podrá seleccionar regresar a una sola partición grande. Por supuesto, a esas alturas, contará con el conocimiento suficiente de ambos sistemas para comprender por qué uno podrá ser mejor que el otro.

Ahora que posee algunos antecedentes acerca del particionamiento en Linux, regresemos al proceso mismo de instalación. Usted debe observar una pantalla como la de la figura 22-4.

En este ejercicio, seleccione la herramienta de particionamiento Disk Druid, la cual le proporciona un mayor control manual sobre sus particiones de disco. Red Hat desarrolló la herramienta de particionamiento Disk Druid como una manera sencilla para crear particiones y asociarlas con los directorios en los que éstas se montarán. Cuando comience Disk Druid, podrá ver todas



Figura 22-4. Seleccionar un método para particionar el disco duro.

las particiones existentes en su disco. Las entradas de cada partición muestran la información siguiente:

- **Mount Point** Aquí es donde se monta la partición. Inicialmente, esta ubicación no debería tener ninguna opción.
- **Device** Linux asocia cada partición con un dispositivo independiente. Para propósitos de instalación, lo único que necesita saber es que en los discos IDE, cada dispositivo comienza con /dev/hdYX, donde X es
  - **a** para cadena principal, disco principal.
  - **b** para cadena principal, disco secundario.
  - **c** para cadena secundaria, disco principal.
  - **d** para cadena secundaria, disco secundario.

  y *Y* es el número de partición del disco. Por ejemplo, /dev/hda1 es la primera partición en la cadena principal, disco principal. SCSI sigue la misma idea básica, excepto que en lugar de comenzar con /dev/hd, cada partición comienza con /dev/sd y sigue el formato /dev/sd*XY*, donde *X* es la letra que representa un drive físico único (**a** es para SCSI id 1, **b** es para SCSI id 2, etc.). La *Y* representa el número de partición. Por tanto, /dev/sdb4 es la cuarta partición del disco SCSI con id 2. El sistema es un poco más complejo que el de Windows, sin embargo, la localización de cada partición es explícita: no más adivinanzas respecto "¿a qué dispositivo físico corresponde E:?".
- **Requested** Éste es el tamaño mínimo requerido cuando se definió la partición.
- **Actual** Ésta es la cantidad de espacio real que se asigna a una partición.
- **Type** Éste es el tipo de partición. El tipo de Linux por omisión es el Linux Native, sin embargo, Disk Druid también entiende muchos otros, dentro de los que se encuentran FAT, VFAT y NTFS.

La segunda mitad de la pantalla muestra los resúmenes de los drives. Cada línea representa un solo drive y sus características. Entre la información que se presenta, se encuentra la siguiente:

- El nombre del drive (sin el /dev/ que le precede).
- La geometría del disco en formato *cilindros/cabezas/sectores.*
- El tamaño total del disco.
- La cantidad de disco que se ha asignado (particionado).
- La cantidad de disco que aún está disponible para particionarse.

En la mitad de la pantalla se encuentran las opciones de menú que usted utiliza para especificar lo que desea hacer con el Disk Druid. Estos botones son los siguientes:

- **Add** Crea una nueva partición.
- **Edit** Modifica los parámetros en la partición resaltada.

- **Delete** Elimina la partición resaltada.
- **Reset** Fija todos los cambios de regreso a sus parámetros originales.
- **Make RAID Device** Comienza el proceso de instalación de una configuración RAID. En cualquier sistema operativo, la instalación de una configuración RAID no es algo trivial y tiene implicaciones que no siempre son obvias. Esta opción está más allá del alcance de este capítulo.
- **Next** Lleva a cabo los cambios en el disco.
- **Back** Elimina todos los cambios realizados utilizando el Disk Druid y sale del programa.



NOTA El programa no lleva a cabo en el disco cualquier modificación que usted haya hecho dentro del Disk Druid hasta que haga clic en el botón Next.

Agregar una partición

Para crear una nueva partición, haga clic en el botón New. Esto hace que aparezca una caja de diálogo parecida a la de la figura 22-5.

Figura 22-5. La caja de diálogo Add Partition.

Los elementos de la caja de diálogo son los siguientes:

- **Mount Point** Este es el directorio donde desea que el programa monte esta partición automáticamente en el momento del arranque.
- **File System Type** Es el formato que utilizará el sistema de archivos en cuestión. En general, ext3 será la mejor opción aquí, a menos que esté configurando un arreglo de discos RAID con base en el software, en cuyo caso puede seleccionar Software Raid de la lista que aparece. También, cuando crea una partición intercambiable, asegúrese de seleccionarle el tipo de sistema de archivos intercambiables.
- **Allowable Drives** Para un sistema con múltiples discos duros, aquí se puede designar en qué drives puede crearse la partición.
- **Tamaño (MB)** Éste es el tamaño de la partición en megabytes.
- **Additional Size Options** En esta caja, puede seleccionar cómo implantará el Disk Druid sus opciones de tamaño. Puede seleccionar Fixed Size, en cuyo caso el tamaño que ingrese en el campo Size (MB) será el que se utilice; o puede seleccionar Fill All Space Up to (MB), lo cual le permite especificar un tamaño máximo, aunque permite que el Disk Druid encuentre el tamaño más apropiado. Por último, puede seleccionar Fill to Maximum Allowable Size, el cual fijará el tamaño de la partición actual al resto del espacio en el disco.

Para crear un esquema simple de partición, siga los pasos siguientes:

1. En el parámetro Partition Type, seleccione Linux Swap.
2. En el campo Size (MB), escriba un valor que sea el doble del tamaño de la RAM instalada en el sistema. (Si lo desea, y el sistema cuenta con una gran cantidad de espacio en disco, puede escribir cuatro veces el tamaño de la RAM instalada).
3. Haga clic en OK para almacenar la información de las particiones intercambiables.
4. Haga clic en el botón Add, de nuevo en el Disk Druid, para agregar una partición final.
5. En la caja de diálogo Add, ingrese una diagonal en el punto de montaje (en el directorio raíz).
6. En tipo de partición, seleccione ext3.
7. En tamaño, ingrese ya sea el espacio en disco restante disponible, o simplemente haga clic en la caja de verificación Fill to Maximum Allowable Size para utilizar de manera automática todo el espacio disponible.
8. Haga clic en OK para guardar la información de la partición raíz.
9. En la pantalla Disk Druid, haga clic en el botón Next para aceptar sus opciones y proceda a formatear las particiones y continúe la instalación.

Como mínimo, necesita contar con dos particiones: una para almacenar todos los archivos (montados como raíz) y la otra para espacio intercambiable. Por lo común, el espacio intercambiable se configura para un tamaño del doble de la RAM disponible si existe menos de 128 MB de RAM o de exactamente la misma cantidad de RAM si existen más de 128 MB. Cuando se tenga

duda, no hay problema en que se asigne más espacio intercambiable del recomendado, dentro de lo razonable.

Otras tareas de manipulación de las particiones Una vez que haya recorrido los pasos para agregar una partición y se sienta a gusto con las variables involucradas (puntos de montaje, tamaños, tipos, dispositivos, etc.), el proceso real de la edición y eliminación de particiones es muy simple. *Editar una entrada* significa simplemente modificar las mismas entradas que usted estableció en el momento de agregar la partición. *Eliminar una partición* requiere solamente que usted confirme que desea llevar a cabo la eliminación.

Instalación de GRUB

GRUB es el administrador de arranque por omisión de Linux. Un *administrador de arranque* maneja el proceso de comenzar la carga de un sistema operativo. Si está familiarizado con Windows NT, es seguro que ya manejó el NT Loader (NTLDR), el cual presenta el menú en el momento del arranque, permitiéndole seleccionar si desea Windows NT o Windows NT (solo VGA). GRUB efectivamente hace lo mismo, pero sin menús tan llamativos.

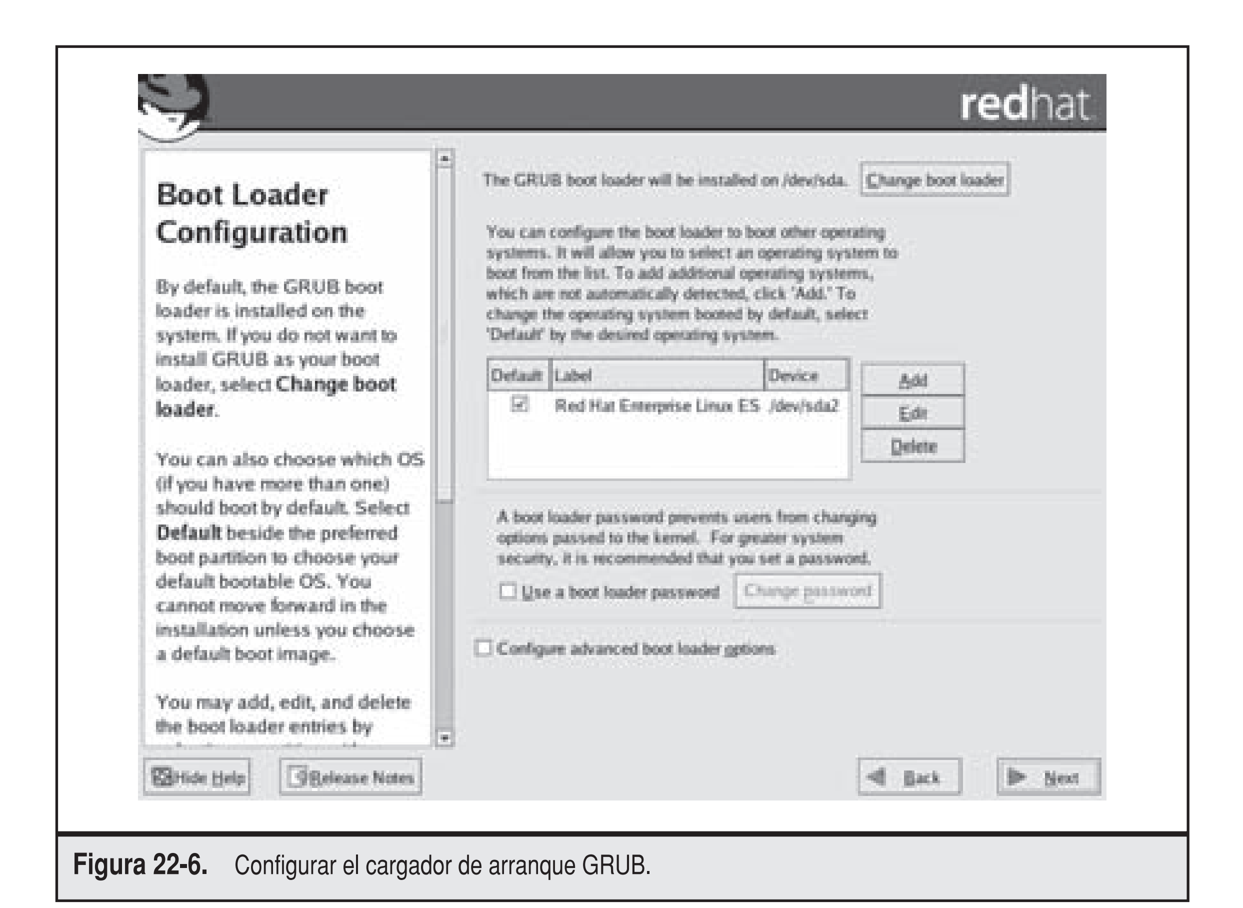


Figura 22-6. Configurar el cargador de arranque GRUB.

Puede configurar la herramienta Red Hat para instalar el GRUB, de manera que arranque múltiples sistemas operativos si así lo desea (vea la figura 22-6). También puede seleccionar no instalar un cargador de arranque (lo cual puede ser útil en ciertas circunstancias). Asimismo, esta pantalla de instalación le permite seleccionar una contraseña para el cargador de arranque, la cual deberá utilizar para proteger los parámetros del sistema de otros usuarios. Puesto que este sistema de ejemplo probablemente será utilizado solo por usted, no es necesario que establezca una contraseña para el cargador de arranque. Haga clic en Next para continuar.

Instalación de la conectividad de redes

Red Hat ya está listo para configurar sus tarjetas de interfase de red (vea la figura 22-7). Cada tarjeta de interfase que tenga se encuentra listada en la parte superior. Los dispositivos de Ethernet aparecen numerados como eth0, eth2, y así sucesivamente. Usted puede configurar cada interfaz ya sea utilizando el DHCP o configurando la dirección IP en forma manual. Si opta por configurarla manualmente, asegúrese de contar con la dirección IP y las direcciones de máscara de red, de red y de difusión.

En la mitad inferior de la pantalla, podrá ver las opciones de configuración para proporcionar a la máquina un nombre de host, una compuerta e información relacionada con el DNS. Una vez que haya llenado todos estos campos, haga clic en Next para continuar.

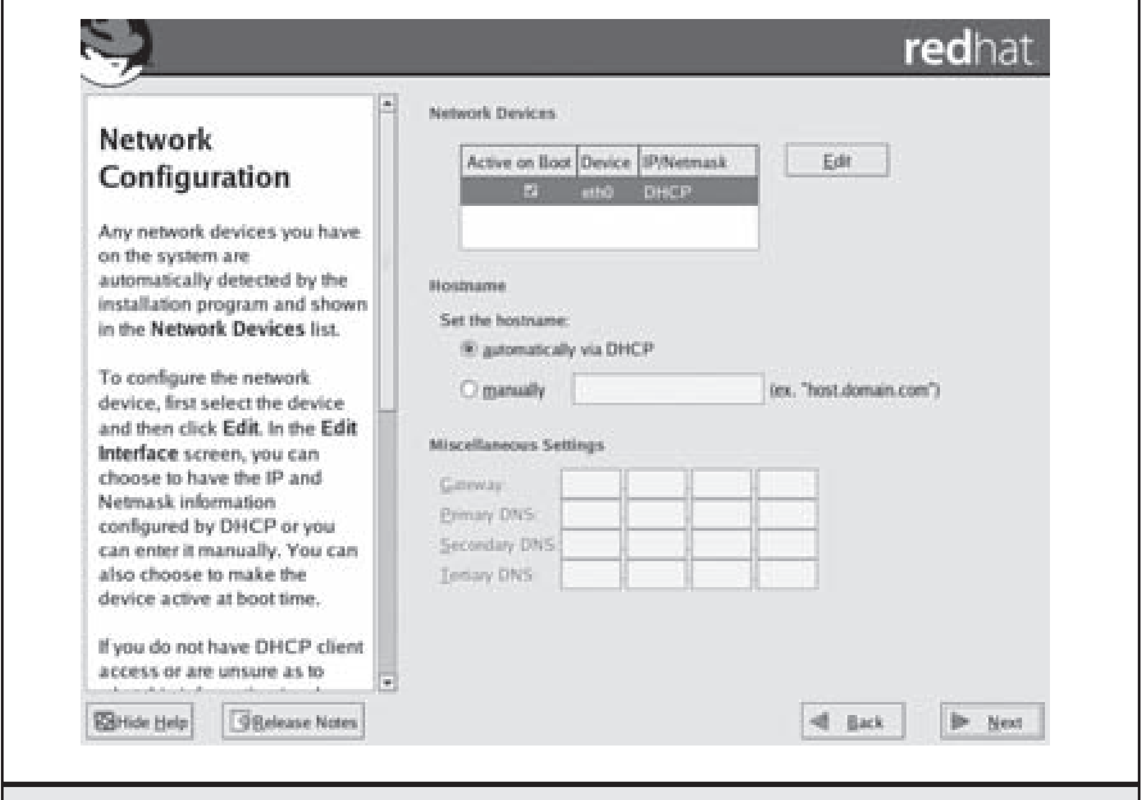


Figura 22-7. Configurar los parámetros de la red durante la instalación.

Configuración de la firewall

Las versiones recientes de Red Hat Linux vienen con un sistema de firewall incorporado basado en software que ayuda a mantener el sistema seguro. La figura 22-8 le muestra las opciones de configuración de la instalación de la pared.

Una vez que habilite firewall incorporada con el botón Enable firewall, puede seleccionar alguna de las opciones siguientes, las cuales permitirán ciertos tipos de tráfico de red entrante a los servicios que desea correr en el servidor. Por ejemplo, si piensa utilizar este servidor para almacenar un servidor web, deberá seleccionar Web Server (HTTP, HTTPS) para permitir dicho acceso al servidor.

En la parte más inferior de la pantalla de configuración de la pared, usted puede seleccionar si habilitar una facilidad llamada Security Enhanced Linux (SELinux o Linux SE). SELinux ofrece

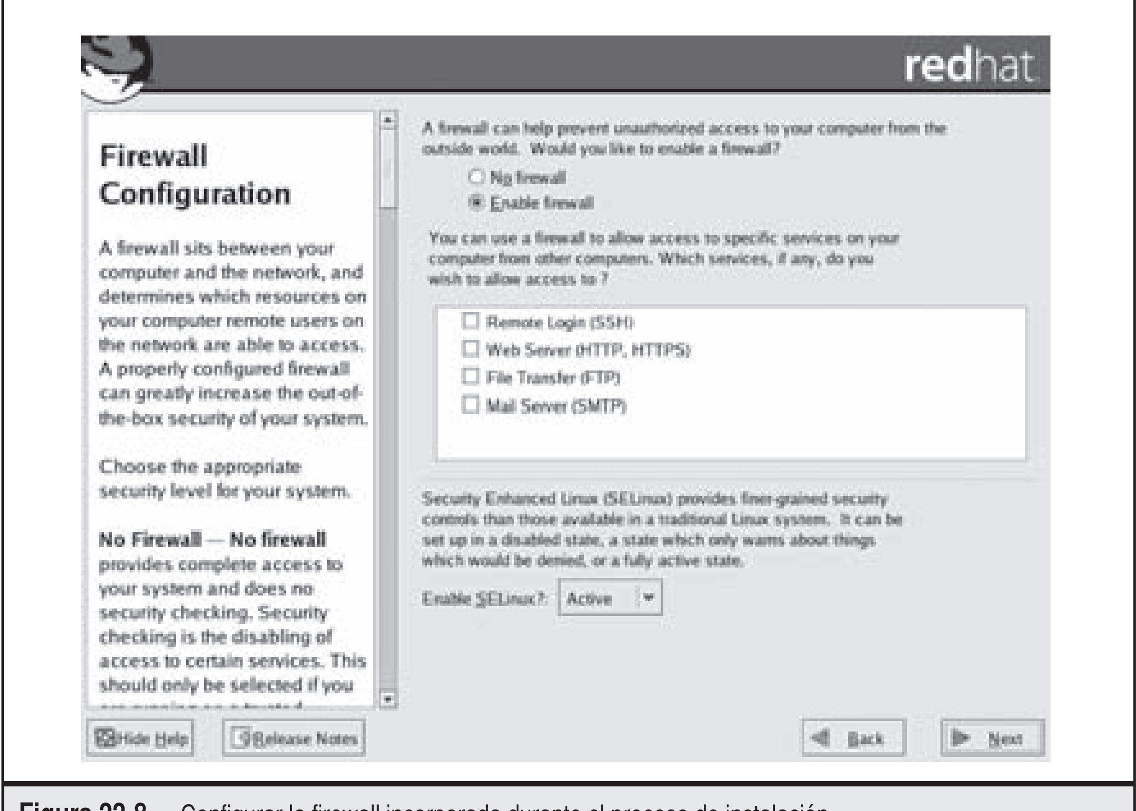


Figura 22-8. Configurar la firewall incorporada durante el proceso de instalación.

un método de control de seguridad más fino para supervisar la actividad de la seguridad. De la caja de diálogo de SELinux, puede seleccionar Disable it, set in to Warn o make it Active. Seleccione la opción make it Active y oprima Next para continuar.

Agregar idiomas

Ahora, el programa de instalación le solicitará que seleccione qué soporte de idioma adicional desea para la instalación. (Vea la figura 22-9). Asegúrese de que ha seleccionado el idioma por omisión adecuadamente, seleccione cualquier idioma adicional que desee utilizar en el servidor y haga clic en Next para continuar.

Configurar el huso horario

La pantalla de configuración del huso horario (vea figura 22-10) le permite seleccionar el huso horario en el que se localiza la máquina. Si el reloj del hardware del sistema lleva el control de la

Figura 22-9. Seleccionar el soporte del idioma adicional por instalar.



Figura 22-10. Configuración del huso horario.

hora en Universal Coordinated Time (UTC), asegúrese de hacer clic en la casilla de verificación System Clock Uses UTC, a fin de que Linux pueda determinar la diferencia entre los dos y desplegar correctamente la hora local.

Crear cuentas

La herramienta Red Hat Installation crea una cuenta llamada *raíz* por usted. Esta cuenta de usuario es de naturaleza similar a la cuenta del administrador de Windows Server: el usuario que tenga permiso para acceder a esta cuenta posee el control total del sistema.

Por tanto, es crucial que proteja esta cuenta con una buena contraseña. Asegúrese de no seleccionar palabras o nombres del diccionario como contraseñas, ya que son fáciles de adivinar.

Para proteger la raíz, no deberá permitir que ingresen como usuario raíz en la red. Esta restricción evita que los intrusos puedan adivinar su contraseña raíz utilizando scripts de ingreso automáticos. Para permitir que los usuarios legítimos se conviertan en el usuario raíz, necesita

ingresar como usted mismo y luego utilizar el comando **su** (*switched user*). Por tanto, configurar la contraseña raíz no es suficiente si desea llevar a cabo la administración remota; también necesita configurar un usuario real.

La configuración de un usuario normal para hacer el trabajo cotidiano es una buena idea. Siguiendo esta práctica, usted se asegura que no va a estropear los archivos de configuración de manera accidental y otros componentes importantes mientras esté navegando por la red o llevando a cabo tareas no administrativas. La excepción a esta regla son ciertas configuraciones de servidor que nunca deben tener usuarios, excepto el usuario raíz —por ejemplo, las firewall.

En el campo Root Password (vea la figura 22-11), ingrese una contraseña segura y difícil de adivinar del usuario raíz. Recuerde que la cuenta raíz es dueña de todo el sistema y puede llevar a cabo cualquier acción, por lo que deberá conservarla en secreto. Confirme su selección de



Figura 22-11. Ingresar la contraseña del usuario raíz.

contraseña en el campo Confirm. Si las dos contraseñas no coinciden *exactamente*, aparecerá una advertencia en la pantalla.

Seleccionar grupos de paquetes

En la pantalla siguiente, Package Installation Defaults (vea la figura 22-12), puede seleccionar los paquetes por instalar en el sistema.

En muchos casos, puede seleccionar las opciones por omisión y continuar, pero si lo desea, también puede seleccionar agregar software adicional a la instalación eligiendo la opción Customize Software Packages to Be Installed y haciendo clic en Next. Red Hat categoriza estos paquetes en varias descripciones de alto nivel. Estas categorías le permiten hacer una selección rápida de qué tipo de paquetes desea instalar e ignora los detalles de manera segura. Usted también puede optar por instalar todos los paquetes que vienen con Red Hat (seleccionando Everything



Figura 22-12. Seleccionar los paquetes por instalar.

en la parte inferior de la lista de los grupos de paquetes), ¡pero tenga muy en cuenta que dicha instalación puede requerir un espacio de aproximadamente 1.5 GB! La figura 22-13 muestra lo que ve cuando selecciona Customize Software Packages to Be Installed.

Si observa las opciones, puede ver el menú de los grupos de alto nivel que Red Hat ofrece. Usted puede solamente seleccionar los grupos que se vean más interesantes, o un grupo y, después, seleccionar dentro de éste al oprimir el botón Details.

Si selecciona el enlace Details junto a un grupo, podrá observar una pantalla similar a la de la figura 22-14. En esta pantalla, puede agregar o eliminar los paquetes dentro del grupo.

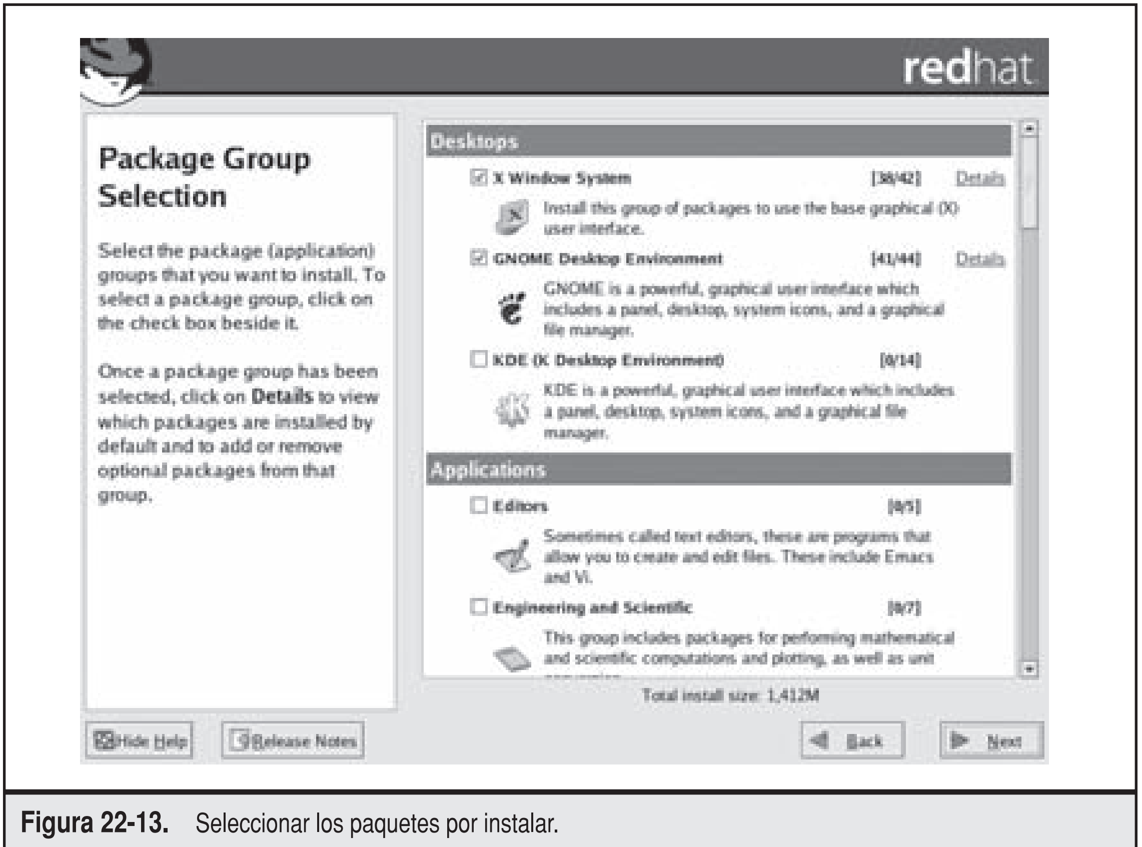


Figura 22-13. Seleccionar los paquetes por instalar.

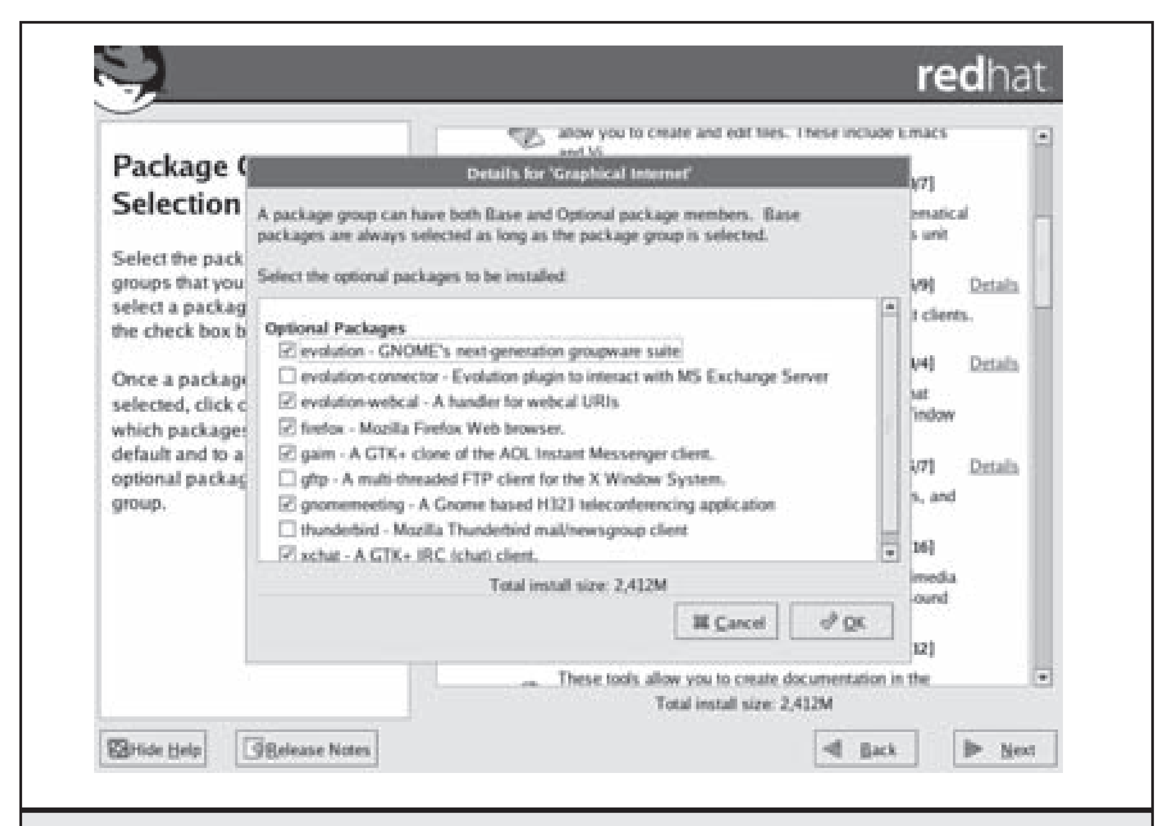


Figura 22-14. Seleccionar los paquetes por instalar dentro del grupo Graphical Internet.

Comenzar la instalación

Ahora verá una pantalla final de confirmación antes de que comience la instalación en serio, como se muestra en la figura 22-15. Si está seguro de que todas sus selecciones son correctas, haga clic en Next para comenzar la instalación. Si fuera necesario, también puede utilizar el botón Back para revisar y modificar cualquiera de las opciones.

En este momento, Red Hat comenzará el proceso de instalación de los paquetes que seleccionó. Dependiendo de la velocidad de su disco duro, CD-ROM y máquina, esta instalación puede



Figura 22-15. Comenzar el proceso de instalación.

tomar de 10 a 20 minutos. Un indicador del estado (vea la figura 22-16) le permite saber cuál es el avance del proceso y cuánto tiempo más le tomará al sistema.

¡Y ya terminó!

¡Eso es todo! El proceso de instalación ya concluyó. El programa lo invita a presionar la tecla para reinicia el sistema. Conforme se reinicia el sistema, asegúrese de que haya quitado cualquier CD-ROM o disco flexible que tenga en su sistema, que pueda arrancar, antes de que lo haga su disco duro.



Figura 22-16. Indicador del progreso de la instalación.

RESUMEN DEL CAPÍTULO

En este capítulo, usted aprendió acerca del proceso de instalar un servidor, seleccionar el hardware correcto, establecer el ambiente apropiado y, por último, instalar el Red Hat Enterprise Linux ES. Todos los comentarios anteriores a este capítulo que estudian el proceso real de instalación de Red Hat Linux se aplican a cualquier servidor que instale, independientemente del sistema operativo.

Los pasos para instalar Red Hat son muy directos. Si alguna vez a sido testigo de procedimiento de instalación de versiones anteriores, habrá notado lo fácil que se ha hecho y cómo se ha reducido el número de opciones de configuración necesarias para comenzar. Lo que hace a Linux muy atractivo es que, a pesar de que esas opciones ya no son parte del proceso de instalación, usted aún puede modificarlas y manipularlas como lo desee una vez que haya terminado de instalarlo y arrancado el sistema.

No olvide consultar las fuentes de información que se listaron en secciones anteriores de este capítulo, por si llegara a necesitar ayuda, y una vez que se convierta en un mago en este tema, no olvide ayudar a los demás.



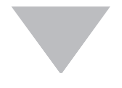
CAPÍTULO 23

Introducción a la administración de los sistemas Linux

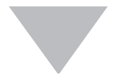
Cuando Linux salió por primera vez en 1991, usted debía ser un administrador de sistemas con mucha experiencia o un buen hacker para utilizar eficazmente el sistema. A pesar de que esta situación resultaba positiva para personas que estaban dispuestas a invertir el tiempo necesario, no lo era para la mayor parte de quienes vieron un gran potencial en el uso de Linux pero que, sin embargo, sabía que la curva de aprendizaje era muy pronunciada.

Por fortuna, las personas en Red Hat (entre otros desarrolladores de Linux), se percataron de esta desventaja e hicieron múltiples esfuerzos para hacer de Linux no solo un software fácil de instalar, sino que también presentara muy pocos problemas para llevar a cabo tareas administrativas básicas.

Este capítulo ofrece un panorama de algunas de las tareas administrativas básicas necesarias para mantener un servidor Linux en operación y que sea de utilidad. Por supuesto, de ninguna manera es una guía completa de la administración de sistemas, pero es un buen comienzo para ir en la dirección correcta. Si después de leerlo está interesado en aprender más acerca de la administración de sistema Linux, consulte la obra *Linux Administration: A Beginner´s Guide*, tercera edición, de Steven Graham. (McGraw-Hill/Osborne, 2002).



NOTA Este capítulo se basa en algunos supuestos. Por ejemplo, supone que ha instalado ya Red Hat Linux y configurado la interfase gráfica de usuario (X Window). También, que usted accedió al sistema y corrió todos los programas como usuario raíz.



PRECAUCIÓN El usuario raíz es muy poderoso bajo Linux. Si está familiarizado con Windows NT, puede pensar del directorio raíz como algo equivalente a la cuenta del administrador. La persona que pueda acceder al directorio raíz tendrá control total al sistema, lo cual incluye la capacidad para destruirlo. Si es principiante en Linux, definitivamente deberá invertir un poco de tiempo para practicar en un sistema independiente antes de empezar a trabajar con los usuarios del sistema.

Este capítulo se divide en dos secciones: la primera trata acerca de la configuración de Red Hat Linux ES con la ayuda de herramientas gráficas para manejar las funciones administrativas del sistema.

La segunda parte se refiere a la interfase de línea de comandos. A pesar de que esta sección no trata el tema de administración de sistemas como tal, es la base para llevar a cabo las tareas básicas de esta actividad. En general, encontrará que la sección acerca del uso de las herramientas gráficas está mucho más orientada hacia instrucciones como "marque con el cursor aquí, haga clic aquí, teclee información aquí, y haga clic en Accept", mientras que la sección de línea de comandos es verbalmente mucho más descriptiva y explica el propósito de los comandos. El capítulo incluye esta sección ya que suponemos que está familiarizado con las facilidades de alto nivel de Linux (como el DNS y su teoría de operación), pero no con las particularidades de la línea de comandos de Linux.

CONFIGURACIÓN DE RED HAT LINUX ES

Las herramientas para la configuración son las bases de la mayor parte de las tareas administrativas que necesitará llevar a cabo. Estas herramientas se encargan de la administración de los usuarios, de la red, de los discos, etc. Lo que hace que estas herramientas sean especialmente

útiles es que brindan una interfase muy congruente para las tareas administrativas de Linux. La única desventaja es que, como otras GUI, tiene ciertas limitaciones. Usted podrá darse cuenta de que, para llevar a cabo las tareas más avanzadas, tendrá que utilizar la interfase de línea de comandos.

ADMINISTRACIÓN DE LOS USUARIOS

Para sacar mayor provecho de la naturaleza multiusuario de Linux, usted necesita agregar, editar y quitar usuarios del sistema, tareas que puede llevar a cabo por medio del programa User Manager.

1. Para abrir el programa User Manager, acceda al menú Applications, seleccione System Settings y después Users and Groups, luego podrá ver la ventana de programa que se muestra en la figura 23-1.
2. Haga clic en el botón Add User que aparece en la parte superior de la ventana del programa. Este comando presenta la caja de diálogo Create New User que se muestra en la figura 23-2.

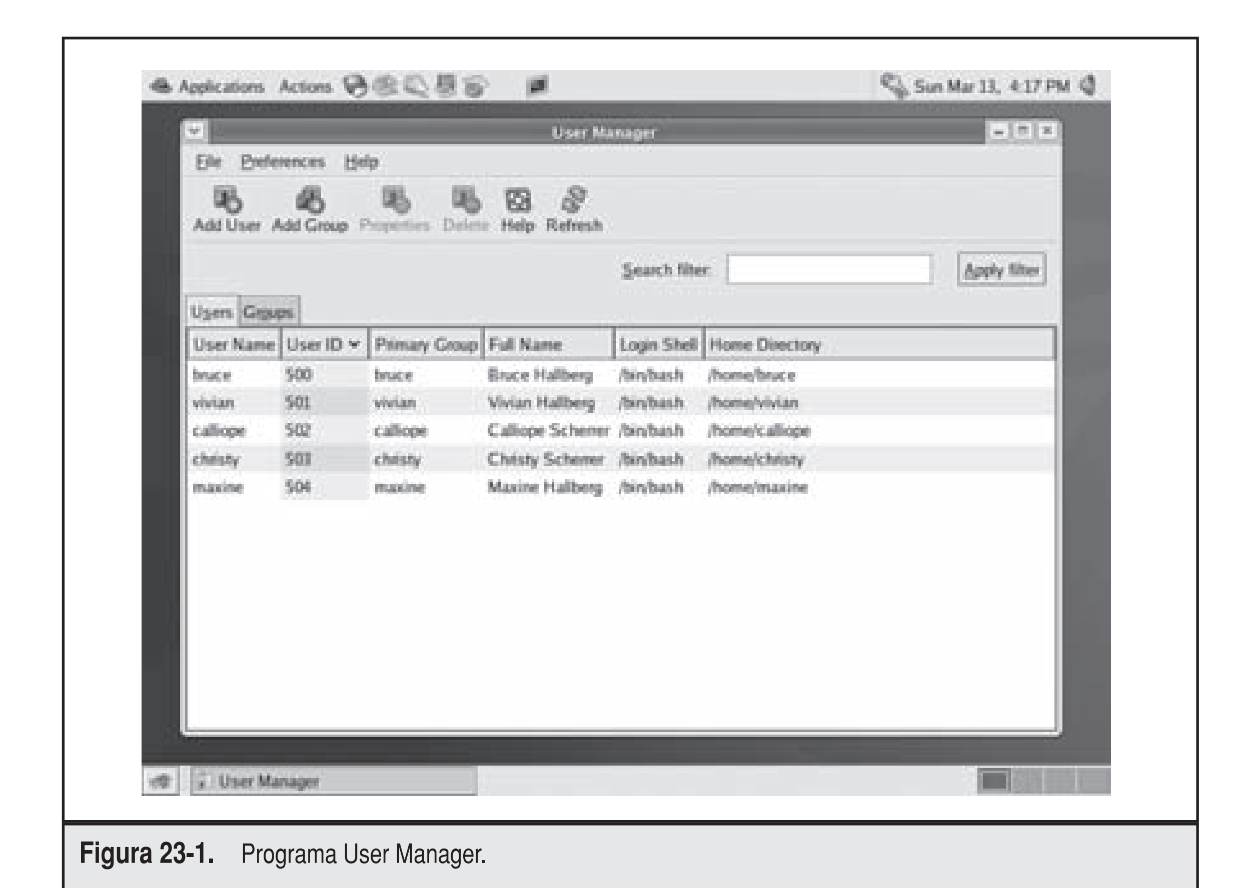


Figura 23-1. Programa User Manager.

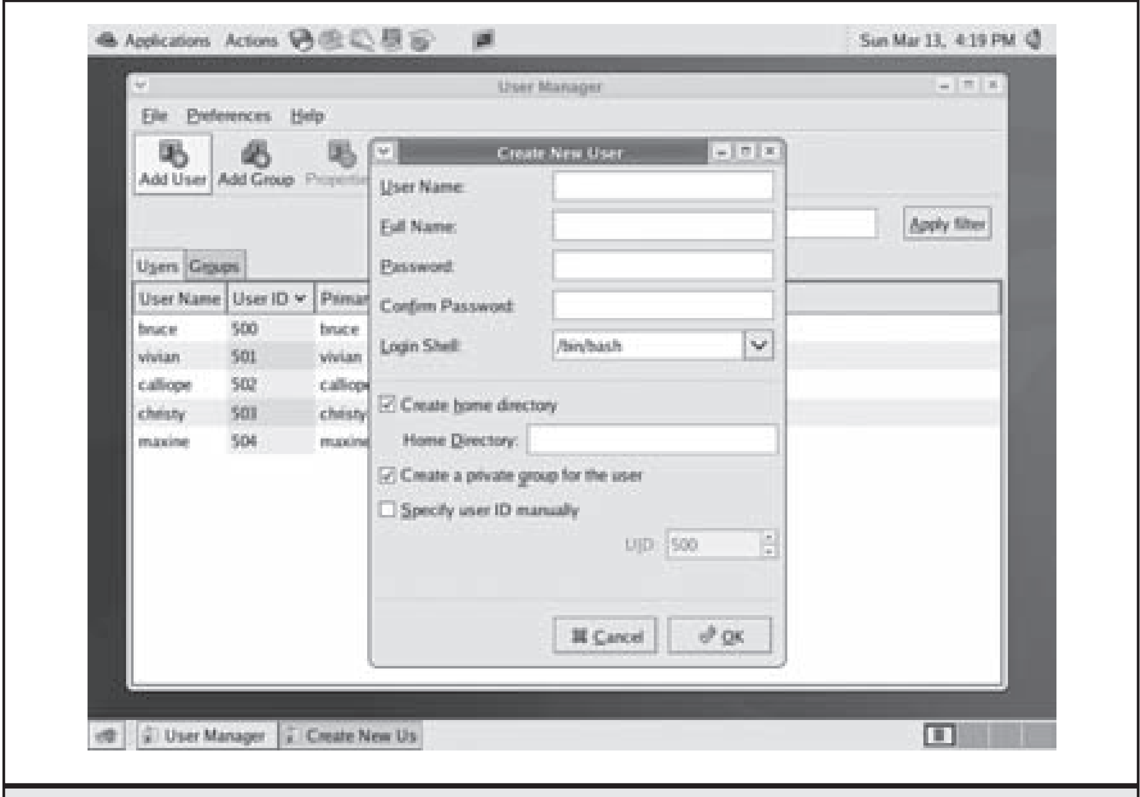


Figura 23-2. Caja de diálogo Create New User.

3. En la caja de diálogo Create a New User deberá, al menos, llenar el espacio del nombre y la contraseña del usuario. La caja de diálogo llenará automáticamente el directorio raíz del usuario y el tipo de shell, opciones que puede aceptar por omisión. Haga clic en OK para crear la cuenta del usuario.
4. Una vez que la cuenta se ha creado, puede hacer doble clic en ella en la lista de cuentas de usuario a fin de configurar algunas propiedades adicionales de la cuenta por medio de la caja de diálogo User Properties que se muestra en la figura 23-3.
5. La pestaña User Data le permite modificar el nombre de usuario, contraseña, directorio raíz y el shell login. Mediante la pestaña Account Info puede configurar la fecha de expiración del usuario, si así lo desea, y también bloquear su cuenta si esto fuere necesario por alguna razón. La pestaña Password Info le sirve para establecer parámetros relacionados con la expiración de la contraseña de la cuenta de usuario que seleccionó. Por último, la pestaña Groups le permite asignar la membresía de grupo de seguridad de la cuenta de usuario seleccionada.

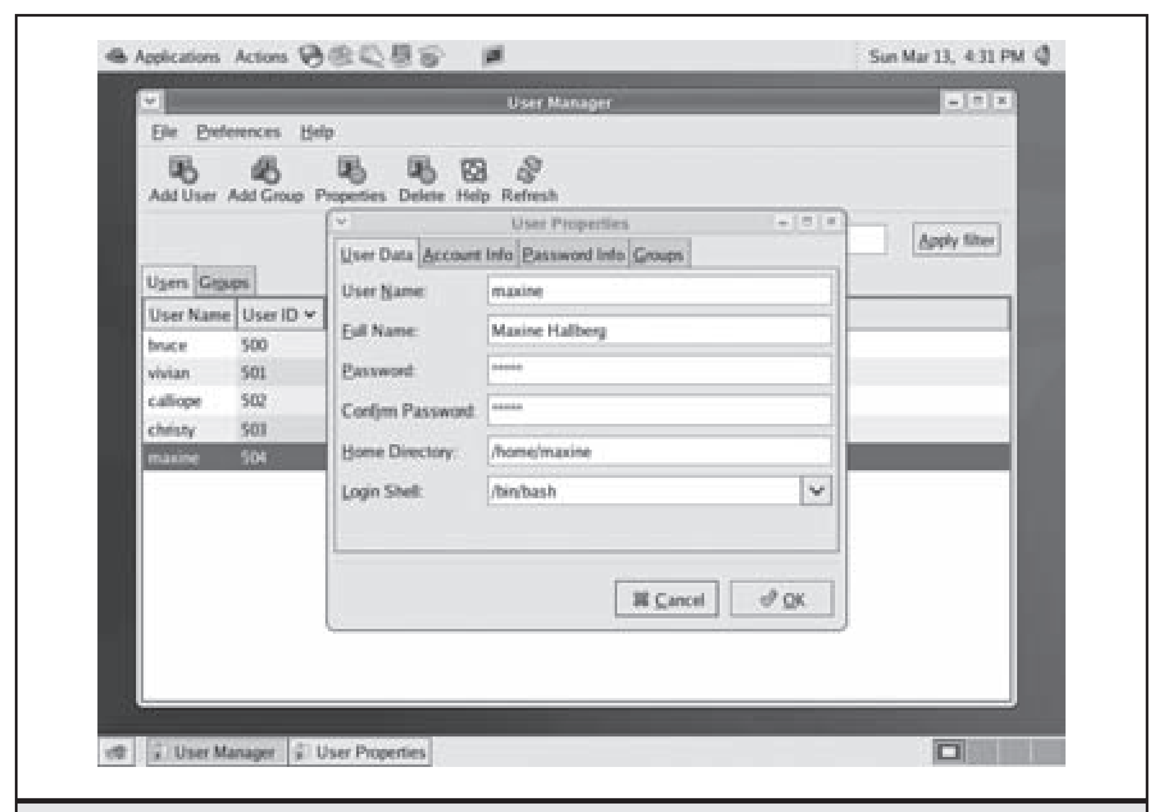


Figura 23-3. Caja de diálogo User Properties.

PISTA Elegir una buena contraseña no significa seleccionar una palabra del diccionario (lo cual incluye palabras en otro idioma), sin importar lo caprichosa o extraña que pueda parecer. Muchos hackers que tratan de ingresar a los sistemas utilizan programas automatizados que cuentan con diccionarios de gran tamaño en muchos idiomas que revisan cada palabra, una a la vez, para probar si alguna de ellas coincide con la contraseña. Una técnica eficaz para seleccionar contraseñas es utilizar una frase y luego considerar la primera letra de cada palabra que compone la frase. Por ejemplo, "Snacking on Oatmeal Squares is good for you" se traduce como SoOSigfy. La frase es fácil de recordar, aun si la contraseña es muy difícil de encriptar. En realidad, su naturaleza críptica hace que SoOSigfy sea una buena contraseña. Otra excelente estrategia para seleccionar contraseñas es tomar una palabra de seis letras o más y, después, sustituir dos o más letras por números. Por ejemplo, la contraseña le77ers (en lugar de letters) es una contraseña muy buena. Por supuesto que las contraseñas son aún mejores a medida que tienen más caracteres.

Para quitar a un usuario, comience en la pantalla User Manager, seleccione la cuenta de usuario que se va a eliminar y haga clic en el botón Delete en la parte superior de la ventana del programa.

CAMBIO DE LA CONTRASEÑA DEL DIRECTORIO RAÍZ

Como se mencionó anteriormente, el usuario raíz es un usuario especial que tiene muchos privilegios en el sistema. Evidentemente, una cuenta tan poderosa necesita estar protegida por una buena contraseña. Si piensa que alguien ha desentrañado la contraseña *raíz* o que alguien la tenía en su poder, (por ejemplo, un exempleado), deberá cambiarla de inmediato. El procedimiento siguiente le muestra cómo modificar la contraseña raíz de un sistema.

1. Primero, abra el menú Applications, seleccione System Settings y después escoja Root Password del menú. Usted verá la caja de diálogo que se muestra en la figura 23-4.

2. Ahora, puede ingresar la nueva contraseña para usar la cuenta raíz en los dos campos que se proporcionan. El programa no le permitirá modificar la contraseña raíz si ambos palabras no coinciden exactamente. (Recuerde que el Red Hat Linux ES, como todos los sistemas operativos de UNIX, utiliza contraseñas que distinguen entre mayúsculas y minúsculas). Haga clic en OK para terminar este cambio.

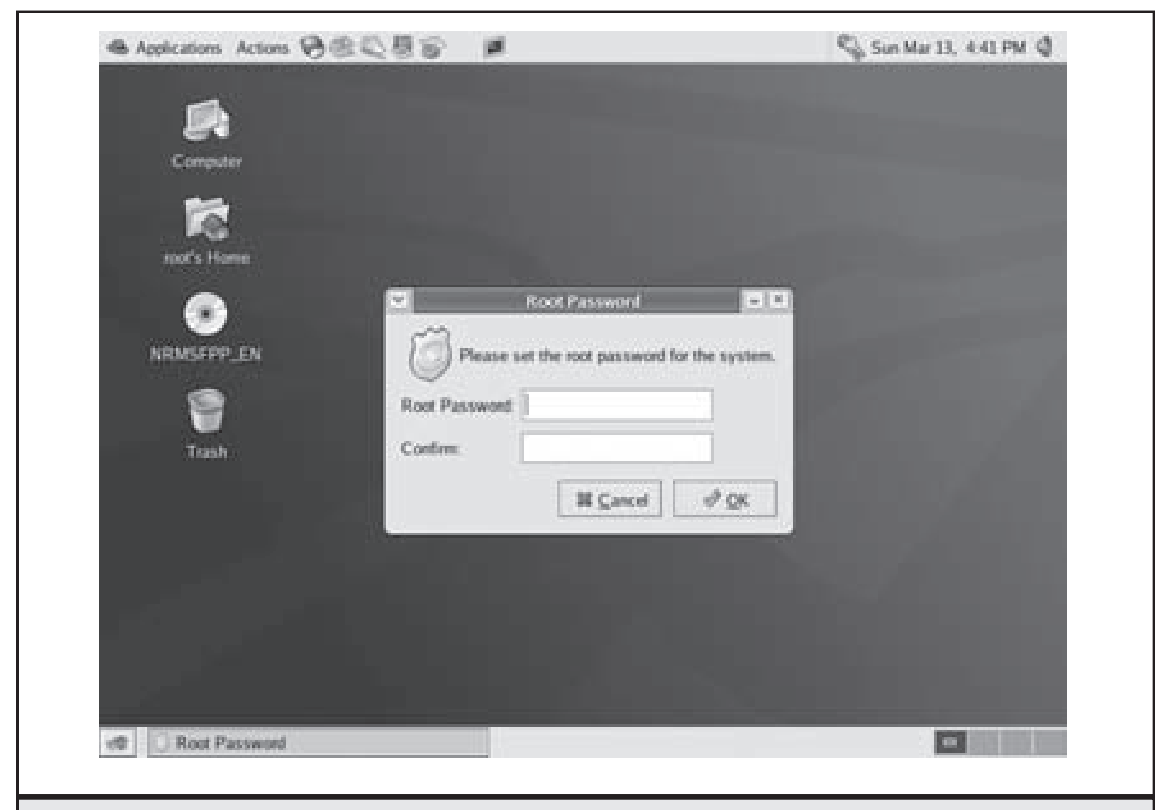


Figura 23-4. Caja de diálogo Root Password.



CONFIGURACIÓN DE LOS PARÁMETROS NORMALES DE LA RED

Linux está muy familiarizado con el ambiente de conectividad de redes. En realidad, su diseño, desde un principio, soporta el uso en un ambiente de red. Las redes son dinámicas y las cosas cambian, y es muy fácil que Linux cambie con ellas. En esta sección se explica cómo cambiar la configuración de red en Linux.

Cambio de su dirección IP

Para modificar la dirección IP de su sistema, siga los pasos siguientes:

1. Abra el menú Applications, seleccione el System Settings y, después, seleccione Network del menú. Usted verá la caja de diálogo Network Configuration que se muestra en la figura 23-5.
2. Haga clic en el botón Edit en la parte superior de la caja de diálogo Network Configuration, luego aparecerá la caja de diálogo Ethernet Device que se muestra en la figura 23-6.

Figura 23-5. Caja de diálogo Network Configuration.

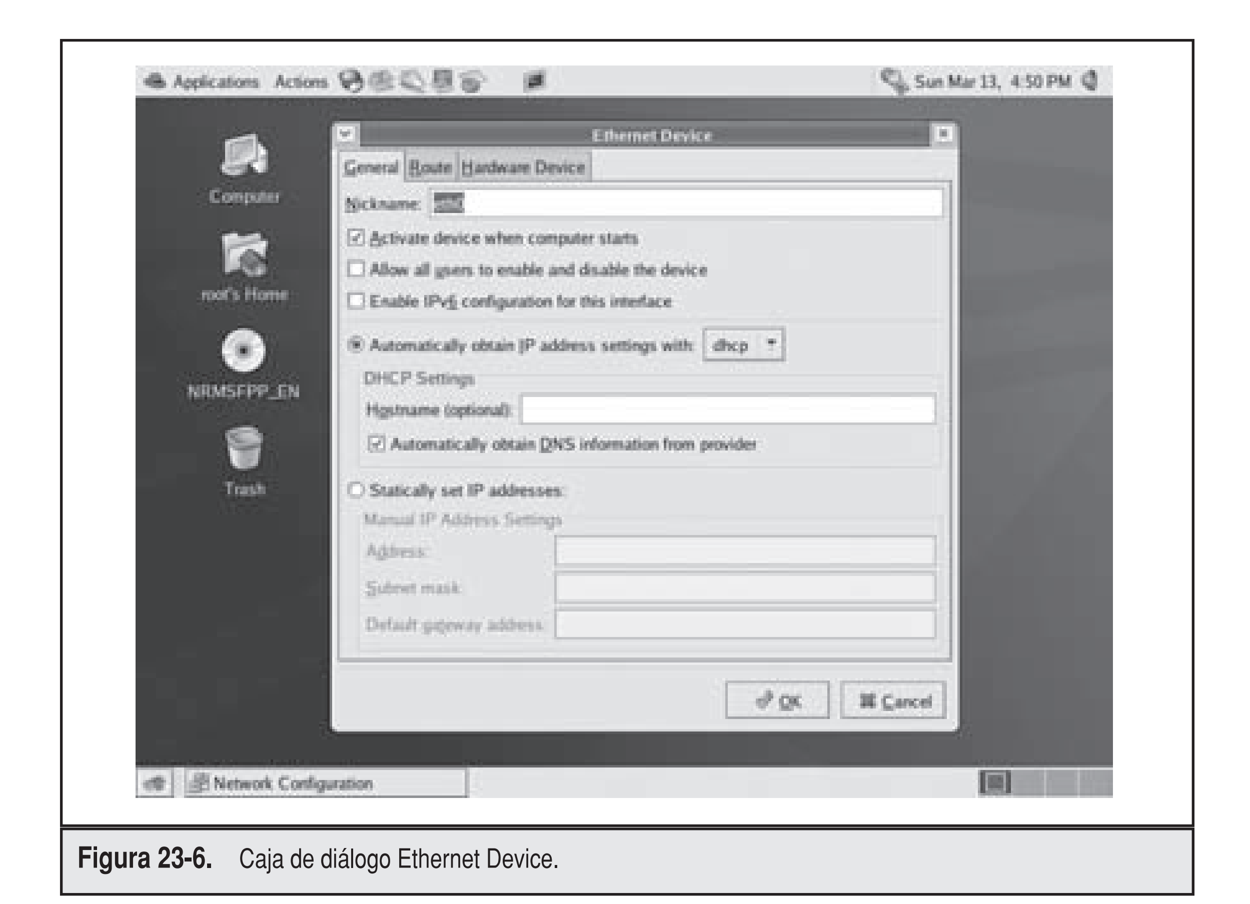


Figura 23-6. Caja de diálogo Ethernet Device.

3. En la mayoría de los casos, si un sistema está configurado para utilizar el DHCP para obtener su dirección IP, usted no deberá cambiar los parámetros. Sin embargo, a veces necesitará configurar una dirección IP estática en un sistema. Para hacerlo, primero haga clic en la opción Statically Set IP Addresses y, después, podrá ingresar la información apropiada de dirección IP en los campos Manual IP Address Settings.
4. Una vez que haya efectuado todas las selecciones, haga clic en OK para aceptar los cambios.

Archivo /etc/hosts

El archivo /etc/hosts contiene una lista de nombres host para los mapeos IP. La mayoría de los sistemas utilizan esta lista para encontrar otras máquinas en la red en caso de que no hubiere acceso al DNS. Dentro de los parámetros típicos se incluyen el host mismo, los servidores para los servicios normales (como el servidor DNS) y los parámetros para las compuertas.

Los pasos para agregar parámetros al archivo /etc/hosts/ son los siguientes:

1. Abra el menú Applications, seleccione System Settings y después Networks del menú. Usted verá la caja de diálogo Network Configuration que se muestra en la figura 23-5.
2. Haga clic en la pestaña Hosts, que se muestra en la figura 23-7.
3. Haga clic en el botón New para agregar un nuevo parámetro. Usted verá la caja de diálogo Add/Edit Hosts Entry que se muestra en la figura 23-8.
4. Ingrese la información adecuada en los campos Address and Hostname y, si lo desea, en el campo Aliases.

Cambio de la configuración del cliente DNS

Si su sistema necesita trabajar con una red más grande (como Internet), es una buena idea configurar sus sistema para que cuente con un servidor DNS, lo que le permitirá traducir los nombres de host en direcciones IP y viceversa. Muchas veces, los servidores DNS apropiados se asignan de manera automática a través del proceso DHCP, pero, si fuere necesario, usted puede controlar

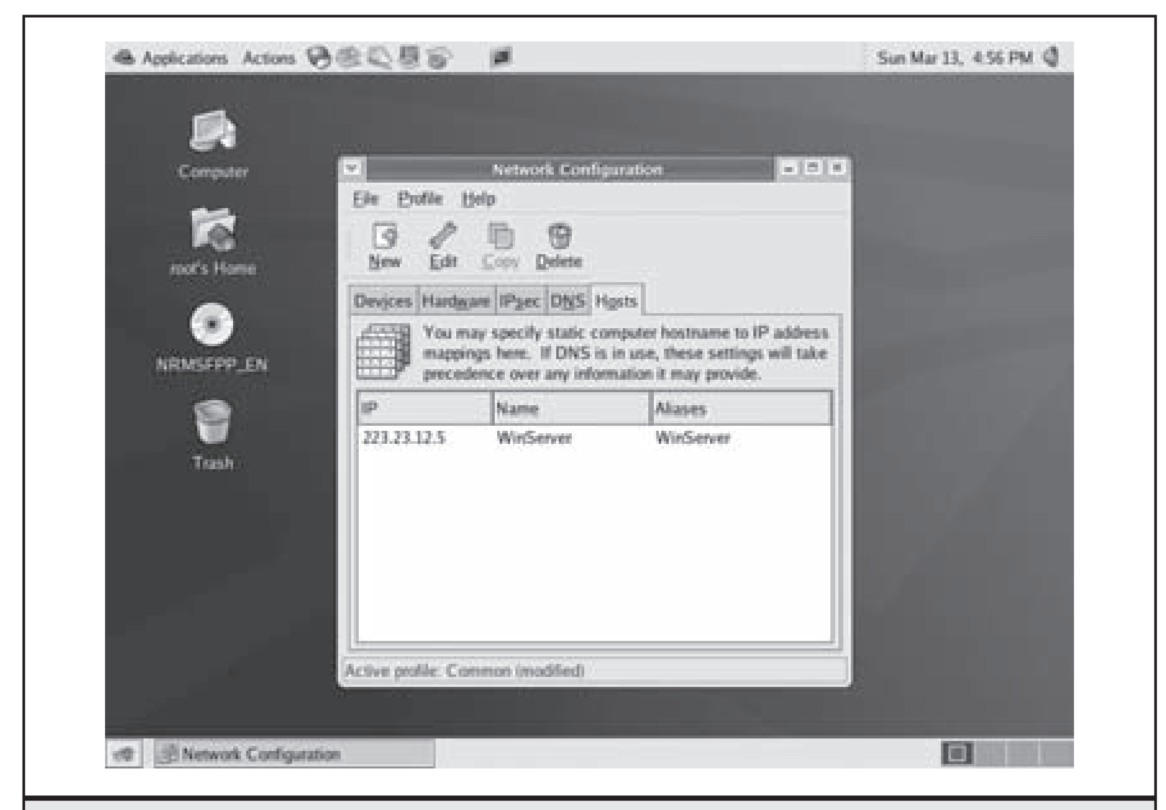


Figura 23-7. Modificación de las entradas Host con la caja de diálogo Network Configuration.

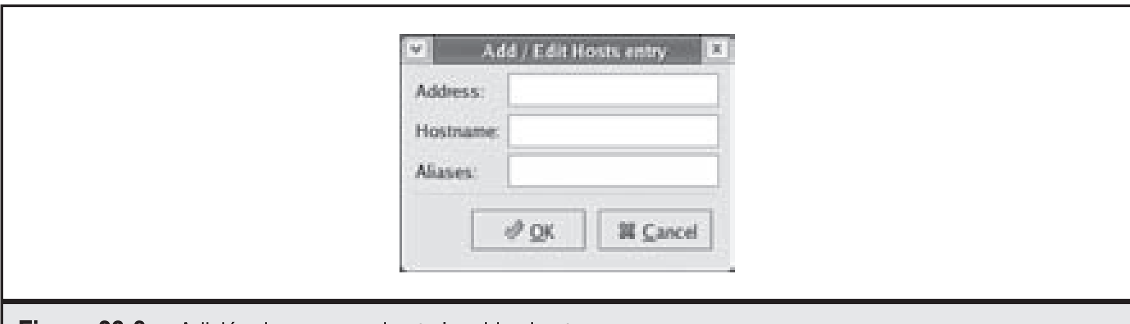


Figura 23-8. Adición de un nuevo host al archivo hosts.

estos parámetros mediante el empleo de la caja de diálogo Network Configuration. Siga los pasos siguientes:

1. Abra el menú Applications, seleccione System Settings y después seleccione Network del menú. Usted verá la caja de diálogo Network Configuration que se muestra en la figura 23-5.
2. Haga clic en la pestaña DNS en la caja de diálogo Network Configuration para desplegar la configuración del DNS de la computadora, como se muestra en la figura 23-9.
3. Ingrese las direcciones IP de los servidores DNS que desee utilizar en los campos DNS principal, DNS secundario y DNS terciario.
4. Cierre la caja de diálogo Network Configuration para aceptar estos cambios.

FUNDAMENTOS DE LA LÍNEA DE COMANDOS DE LINUX

Históricamente, el aspecto de UNIX que lo hace más poderoso y flexible ha sido las opciones disponibles a través de la línea de comandos. A menudo, los observadores esporádicos de los gurúes del UNIX se sorprenden por la forma en que unos cuantos comandos tecleados cuidadosamente pueden dar como resultado acciones tan drásticas. Desafortunadamente, este poder se logra a costa de la facilidad de uso. Por esta razón, las GUI han proliferado tanto y se han convertido en el estándar *de facto* de muchas herramientas.

Sin embargo, a medida que acumule más experiencia, se dará cuenta de que es difícil que las GUI presenten todas las opciones disponibles a un usuario, ya que hacerlo haría que la interfase fuera tan complicada como el equivalente en línea de comandos. Por tanto, las GUI se han mantenido muy simplificadas y los usuarios que cuentan con mayor experiencia han tenido que utilizar la línea de comandos.



PISTA Antes de que se involucre en una guerra sobre "qué interfase es mejor", recuerde que ambos tipos sirven para un propósito, y que cada una tiene sus beneficios así como sus debilidades. Al final, la persona que opte por tener el dominio de las dos, saldrá beneficiado.

Figura 23-9. Configuración de los parámetros DNS del sistema.

Antes de ir a los detalles de la interfase de línea de comandos de Linux, debe recordar que esta sección está muy lejos de ser un estudio exhaustivo de las herramientas. En lugar de tratar de abarcar muchas herramientas sin profundizar en ellas, esta sección explica en detalle una cantidad más reducida de herramientas que son cruciales para el trabajo cotidiano.



NOTA Todos los comandos que se estudian en esta sección se representarán en una ventana terminal. Usted puede acceder a una ventana terminal si abre el menú Applications, luego el menú System Tools y, después, selecciona Terminal del menú. Este comando despliega una leyenda similar a [root@*hostname*/root]#, donde el hostname es el nombre de su máquina.

Variables de ambiente

El concepto de variables de ambiente es casi el mismo en Windows que en UNIX. La única diferencia estriba en la forma en que usted configura, ve y quita las variables.

Impresión de las variables de ambiente

Para que aparezcan todas sus variables de estado, utilice el comando **printenv**, como en el ejemplo siguiente:

```
[root@ford /root]# printenv
```

Para mostrar una variable de ambiente específica, identifique la variable como un parámetro en **printenv**. Por ejemplo, para ver la variable de estado USER, usted deberá teclear:

```
[root@ford /root]# printenv USER
```

Establecimiento de variables de ambiente

Para establecer una variable de ambiente, utilice el formato siguiente:

```
[root@ford /root]# variable=value
```

donde *variable* es el nombre variable y *value* es el valor que usted desea asignarle a la variable. Por ejemplo, para fijar la variable de ambiente FOO a un valor BAR, tendría que teclear lo siguiente:

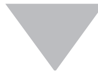
```
[root@ford /root]# FOO=BAR
```

Después de asignar el valor, utilice el comando **export** para finalizarlo. El formato del comando **export** es el siguiente:

```
[root@ford /root]# export variable
```

donde *variable* es el nombre de la variable. En el ejemplo donde se asignó la variable FOO, usted tendría que teclear lo siguiente:

```
[root@ford /root]# export FOO
```



PISTA De la manera siguiente, puede combinar los pasos para fijar la variable de estado con el comando **export**:

```
[root@ford /root]# export FOO=BAR
```

Si el valor de la variable de ambiente que desea asignar contiene espacios, necesita poner la variable entre comillas. En el ejemplo anterior, si usted hubiera querido fijar FOO a “Welcome to the BAR of FOO”, hubiera tenido que teclear lo siguiente:

```
[root@ford /root]# export FOO="Welcome to the BAR of FOO."
```

Eliminación de variables de ambiente

Para eliminar una variable de ambiente, utilice el comando **unset**:

```
[root@ford /root]# unset variable
```

donde *variable* es el nombre de la variable que usted desea eliminar. Por ejemplo, para eliminar la variable de estado FOO, usted debe teclear lo siguiente:

```
[root@ford]# unset FOO
```

Diferencias entre las líneas de comandos

Una de las dificultades para mover la interfase de línea de comandos, especialmente si está acostumbrado a utilizar las herramientas, como el cmd.exe de Windows, es lidiar con un shell que tenga un gran número de atajos que puedan sorprenderlo si no es lo suficientemente cuidadoso. Esta sección estudia las diferencias más comunes y explica por qué se comportan de la manera en que lo hacen.

Expansión del nombre del archivo

En los shell que se basan en UNIX, como bash, usted expande comodines que se ven en la línea de comandos *antes* de incluirlos como parámetros en la aplicación. Esto contrasta mucho con el modo de operación por omisión de las herramientas basadas en DOS, las cuales a menudo tienen que llevar a cabo su propia expansión de comodines. Esto también significa que debe ser especialmente cuidadoso cuando utiliza los caracteres comodines.

Por sí mismos, los caracteres comodines son idénticos a los del command.com. El asterisco (*) se compara con todos los nombres de archivo, mientras que el signo de interrogación (?) se compara con los caracteres individuales. Si necesita utilizar estos caracteres como parte de otro parámetro, puede evitarlos si coloca una diagonal invertida (\) enfrente de ellos. Este caracter tendrá como efecto que el shell interprete un comodín simplemente como otro caracter.

Variables de ambiente como parámetros

Aunque el command.com le permite efectuar la misma operación, generalmente no es muy común hacerlo y, por tanto, a menudo se olvida. Usted puede utilizar las variables de ambiente como parámetros en la línea de comandos. Esto significa que la generación del parámetro $FOO dará como resultado transferir el valor de la variable de estado FOO en lugar de la cadena "$FOO".

Comandos múltiples

En el shell bash, es posible ejecutar múltiples comandos en la misma línea separándolos con un signo de punto y coma (;). Por ejemplo, suponga que desea ejecutar la siguiente secuencia de comandos en una sola línea:

```
[root@ford /root]# ls -l
[root@ford /root]# cat /etc/hosts
```

En lugar de ello, pudo haber tecleado lo siguiente:

```
[root@ford /root]# ls -l ;cat /etc/hosts
```

Acentos invertidos

Usted puede hacer que la salida de un programa sea el parámetro de otro. ¿Qué salvajada es ésta? ¿Suena raro? Bueno, ya es hora de acostumbrarse, pues ésta es una de las facilidades disponibles en todos los shells de UNIX, que se utilizan de la manera más creativa.

Un acento invertido (`) le permite incrustar comandos como parámetros de otros. Un caso común del uso de este carácter es para transferir un número de un archivo como un parámetro del comando **kill**. Un ejemplo típico ocurre con el *named* del servidor DNS. Cuando este servidor se inicia, escribe el nombre de identificación del proceso en el archivo /var/run/named.pid. Por tanto, la forma genérica de matar al proceso *named* es consultar el número en /var/run/named.pid mediante el comando **cat** y, después, generar el comando **kill** con ese valor, como en el ejemplo siguiente:

```
root@ford /root]# cat /var/run/named.pid
253
[root@ford /root]# kill 253
```

Un problema que se presenta cuando se mata al proceso *named* de esta forma es que no puede automatizar la muerte; cuenta con que una persona leerá el valor en /var/run/named.pid, de forma que ella puede matar el número. El segundo problema no lo es tanto como una molestia: toma dos pasos parar el servidor DNS.

Sin embargo, si utiliza acentos invertidos, puede combinar estos pasos en uno *y* hacerlo en la forma que pueda automatizarlo. La versión de acentos invertidos es similar al ejemplo siguiente:

```
[root@ford /root]# kill 'cat /var/run/named.pid'
```

Cuando el shell bash ve este comando, correrá primero **cat** /var/run/named.pid y almacenará el resultado. Enseguida correrá el comando **kill** y pasará el resultado almacenado a él, todo en un solo paso.

Herramientas para documentar

Linux contiene dos herramientas extremadamente poderosas para hacer accesible la documentación: man e info. En la actualidad, los dos sistemas cuentan con muchas cosas y aplicaciones en común debido a que pueden mover su documentación al formato info. Info se considera superior a man debido a que permite que la documentación se hiperenlace entre sí en una forma parecida a como se encuentra en la World Wide Web, sin tener que escribirse en formato HTML. Por otro lado, el formato man ha funcionado por décadas. Miles de utilidades cuentan solo con una fuente de documentación, que son sus páginas man. Además, múltiples aplicaciones continúan liberando su documentación en formato man puesto que muchos otros sistemas operativos, parecidos a UNIX, como el Sun Solaris, tiene por omisión el formato man para su documentación. Como resultado, ambos sistemas existirán aún por mucho tiempo. Es altamente recomendable estar acostumbrado a trabajar con ambos.

El comando man

Las páginas man (abreviatura de *manual*) son documentos que se encuentran en línea que abarcan el uso de herramientas y sus correspondientes archivos de configuración. El formato del comando **man** es como sigue:

```
[root@ford /root]# man program_name
```

donde el *program_name* es el nombre del programa del cual desea leer la página manual. Observe el ejemplo siguiente:

```
[root@ford /root]# man ls
```

Mientras lea acerca de UNIX y las fuentes de información relacionadas con este sistema (como los grupos de noticias), podrá encontrar referencias a comandos seguidos de números entre paréntesis [como "ls(1)"]. El número representa la *sección* de las páginas del manual, pues cada sección abarca varias áreas del tema. Los números de sección están a la mano para algunas herramientas, como los printf, que son tanto comandos en lenguaje de programación C, como comandos de la línea. Por tanto, existirán dos opciones de dicho comando en dos secciones diferentes.

Para referirse a una sección específica, simplemente especifique el número de sección como primer parámetro y, después, el comando como segundo parámetro. Por ejemplo, para obtener la información de los programadores de C acerca de printf, necesita teclear lo siguiente:

```
[root@ford /root]# man 3 printf
```

Sin embargo, para obtener la información en línea de comandos, debe teclear

```
[root@ford /root]# man 1 printf
```

Por omisión, la página manual del número de sección más bajo se imprime primero.

Los significados de los números de sección son los siguientes:

Número de sección	Significado
1	User tools
2	System calls
3	C library calls
4	Device driver-related information
5	Configuration files
6	Games
7	Packages
8	System tools



PISTA Una opción a la mano del comando man es **–k**. Con esta opción, **man** buscará la información de resumen de todas las páginas man y listará qué páginas coinciden con su número de sección. Por ejemplo, el comando siguiente encontrará páginas que coincidan con el criterio de búsqueda "printf":

```
[root@ford /root]# man -k printf
```

El comando info

Además de las páginas man (relativas al comando anterior man), las páginas info son otra forma común de documentación. Establecidas como el estándar GNU, info es un sistema de documentación muy similar a la web, en el sentido que los documentos pueden ser vinculados entre sí mientras que las páginas man son documentos independientes estáticos. Por tanto, info tiende a ser más fácil de leer, de seguir y de encontrar información.

Para leer los documentos info en una herramienta o aplicación específicos, simplemente invoque info con el parámetro y especifique el nombre de la herramienta. Por ejemplo, para leer acerca de emacs, simplemente teclee lo siguiente:

```
[root@ford /root]# info emacs
```

En general, en primer lugar querrá verificar si existe una página man. Ello se debe a que hay una cantidad mucha mayor de información disponible en el formato man que en el formato info. Algunas páginas man especifican explícitamente que las info tienen un mayor peso y deben ser leídas.

Listas, propiedad y permisos de los archivos

La administración de archivos en Linux es diferente a la de Windows. Esta sección analiza las herramientas necesarias para llevar a cabo la administración básica de archivos. El orden en el que se estudian las herramientas no es muy usual, ya que la sección comienza con la descripción de algunos comandos y, después, regresa a fin de brindar alguna información relativa a sus antecedentes. En realidad, esta organización hace que algunos conceptos sean más fáciles de comprender puesto que el texto se puede referir a las herramientas, con las cuales ya debe estar familiarizado.

El comando ls para el listado de archivos

El comando **ls** se utiliza para obtener las listas de todos los archivos contenidos en un directorio. El comando tiene más de 26 opciones, las más comunes de las cuales son las siguientes:

Opción	Descripción
-l	Listado largo. Además del nombre del archivo, muestra el tamaño, fecha/hora, permisos, propiedad e información de grupo.
-a	Todos los archivos. Muestra todos los archivos en el directorio, incluidos aquellos que se encuentran escondidos que comienzan con un punto.
-1	Listas de una sola columna. Presenta todos los archivos en una sola columna.
-R	Recursivo. Recursivamente presenta todos los archivos y subdirectorios.

Usted puede utilizar cualquier combinación de estas opciones. Consulte la página textinfo para obtener una lista completa de las opciones.

Ejemplo: para presentar todos los archivos en un directorio con una lista larga, teclee lo siguiente:

```
[root@ford /root]# ls -la
```

Ejemplo: para listar archivos que no están escondidos en un directorio que comience con A, teclee lo siguiente:

```
[root@ford /root]# ls A*
```

Acerca de los archivos y directorios

En Linux (y UNIX en general), usted podrá encontrar que casi todo se resume en un archivo. Originalmente, los desarrolladores de Linux adoptaron este enfoque para simplificar el trabajo del programador. Por tanto, en lugar de tener que comunicarse directamente con los controladores del dispositivo, usted utiliza archivos especiales (los cuales para la aplicación parecen como cualquier otro archivo) como puentes. Para acomodar todos estos usos de los archivos, existen diferentes tipos de éstos.

Normal Files Los archivos normales son justamente eso: normales. Contienen datos o ejecutables y el sistema operativo no supone nada acerca de sus contenidos.

Directorios Los archivos de directorio son un ejemplo especial de archivos normales, cuyos contenidos indican la ubicación de otros. Entre los archivos a los cuales los directorios apuntan pueden existir otros directorios. Desde un punto de vista cotidiano, no importa mucho que los directorios en Linux 8 (y UNIX) sean realmente archivos, a menos que trate de abrirlos y leer el archivo de directorio en lugar de utilizar aplicaciones existentes para navegar en ellos.

Enlaces conectados Cada archivo del sistema de Linux obtiene su propio *nodo-i* que guarda un registro de los atributos y la ubicación de un archivo ubicado en el disco. Si necesita referirse a un solo archivo utilizando dos nombres de archivo independientes, puede crear un *enlace conectado*. El enlace conectado tendrá el mismo nodo-i que el archivo original y, por tanto, se verá y comportará exactamente como el archivo original. Cada vez que se crea un enlace conectado, se incrementa una *cuenta de referencia*. Cuando se quita un enlace conectado, la cuenta de referencia se reduce. Hasta el momento en el que la cuenta de referencia llegue a un valor de cero, el archivo permanecerá en el disco.

Usted debe observar que no puede haber un enlace conectado entre dos archivos que se encuentren en particiones diferentes. Ello se debe a que el enlace conectado se remite al archivo original por medio de su nodo-i. Un archivo que se remite por un nodo-i en un sistema de archivos se remitirá a otro en otro sistema de archivos.

Enlaces simbólicos A diferencia de un disco duro, que señala un archivo por medio de su nodo-i, un enlace simbólico señala a otro por su nombre. Por tanto, los *enlaces simbólicos* (a menudo abreviados como *symlinks*) pueden señalar archivos localizados en otras particiones o aun en otros controladores de la red.

Dispositivos de bloqueo En razón de que a todos los controladores de dispositivo se accesa por medio de sistemas de archivos, los archivos del tipo *dispositivo de bloqueo* se utilizan como interfase con dispositivos, como los discos. Los tres rasgos que identifican a un dispositivo de bloqueo son: que tienen un número mayor, un número menor y, cuando se observan mediante el comando ls-l, muestran el primer carácter del permiso como *b*. Observe el ejemplo siguiente:

```
[root@ford /root]# ls -l /dev/hda
brw-rw----   1 root     disk       3,   0 May  5  1998 /dev/hda
```

En este caso, la *b* está al comienzo de los permisos del archivo, el 3 es el número mayor y el 0 es el número menor.

El significado del número mayor es que éste identifica qué controlador de dispositivo representa el archivo. Cuando el sistema acceda a este archivo, el número menor se transfiere al controlador de dispositivo como un parámetro para informarle al controlador a qué dispositivo está accediendo. (Por ejemplo, si existen dos puertos seriales, compartirán el mismo controlador de dispositivo y, por tanto, el mismo número mayor, pero cada puerto serial tendrá un solo número menor).

Dispositivos de carácter De manera similar que los dispositivos de bloqueo, los dispositivos de carácter son archivos especiales a los que se puede acceder por medio del sistema de archivos. La diferencia obvia entre los dispositivos de bloqueo y de carácter es que los primeros se comunican con los dispositivos reales en bloques más grandes mientras que los últimos trabajan con un carácter a la vez. (Un disco duro es un dispositivo de bloqueo, mientras que un módem es un dispositivo de carácter). Las características distintivas de un dispositivo de carácter son que sus permisos comienzan con una *c* y el dispositivo tiene un número mayor y menor. Observe el ejemplo siguiente:

```
[root@ford /root]# ls -l /dev/ttyS0
crw-------   1 root     tty        4,  64 May  5  1998 /dev/ttyS0
```

Tuberías nombradas Una tubería nombrada es un tipo especial de archivo que permite la comunicación entre procesos. Mediante el comando **mknod** (que se estudia después en la sección "Administración y manipulación de archivos"), usted puede crear este tipo especial de archivo que un proceso puede abrir para leer y otro proceso puede abrir para escribir, lo cual indica que permite la comunicación entre los dos procesos. Las tuberías nombradas funcionan especialmente bien cuando los paquetes se niegan a tomar la entrada de una tubería de línea de comandos, pero usted cuenta con otro programa al que necesita alimentarle datos pero no con el espacio en disco para un archivo temporal.

Usted puede decir que un archivo es de una tubería nombrada por el hecho de que el primer carácter de su permiso de archivo es una *p*, como en el ejemplo siguiente:

```
[root@ford /root]# ls -l mypipe
prw-r--r--   1 root     root            0 Jun 16 10:47 mypipe
```

chown: cambio de propiedad

El comando **chown** le permite modificar la propiedad de un archivo a alguien más. Solo el usuario raíz puede modificar esta propiedad. (Los usuarios normales no pueden "prestar" o "robar" la propiedad de un archivo). El formato del comando es como sigue:

```
[root@ford /root]# chown [-R] username filename
```

donde *username* es el login del usuario al que desea modificarle la propiedad y *filename* es el nombre del archivo al que se le modificará la propiedad. El nombre del archivo puede también ser un directorio.

La opción **–R** se aplica cuando el nombre del archivo especificado es un nombre de directorio. Éste le dice al comando que descienda recursivamente a través del árbol de directorios y aplique la nueva propiedad no solo al directorio en sí, sino a todos los archivos y subdirectorios contenidos en él.

chgrp: cambio de grupo

chgrp es otra utilidad de línea de comandos que le permite modificar los parámetros de grupo de un archivo. El comando trabaja de una manera muy similar que **chown**. El formato del comando es como sigue:

```
[root@ford /root]# chgrp [-R] groupname filename
```

donde el *groupname* es el nombre del grupo al que usted desea cambiarle el *filename*. El filename puede ser también un directorio.

La opción **–R** se aplica cuando el filaneme especificado es un nombre de directorio. De la misma manera que con **chown**, la opción informa al comando **chgrp** que descienda recursivamente por medio del árbol de directorios y aplique la nueva propiedad no solo al directorio en sí, sino a todos los archivos y subdirectorios que éste contenga.

chmod: cambio de modo

Los permisos se dividen en cuatro partes. La primera es el primer carácter de los permisos. Si el archivo es normal, entonces no tendrá ningún valor y se representará con un guión (-). Si el archivo tiene un atributo especial, se representará con una letra. Los dos archivos especiales en los que usted debe estar más interesado son los directorios que se representan con una *d* y los enlaces simbólicos que se representan con una *l*.

La segunda, tercera y cuarta partes se representan en grupos de tres caracteres. La primera parte es el permiso del propietario del archivo. La segunda es el permiso del grupo. Finalmente, la última parte es el permiso para el mundo. En el contexto de UNIX, el mundo está conformado, simplemente, por todos los usuarios del sistema, sin tomar en cuenta sus parámetros de grupo.

Las letras utilizadas para representar los permisos son los siguientes:

Letras	Significado
R	Read
W	Write
X	Execute

Cada permiso tiene su correspondiente valor. El atributo read es igual a 4, write es igual a 2 y execute es igual a 1. Cuando combina atributos, está agregando sus valores.

La razón por la que estos atributos necesitan en valores es para asegurar que pueda utilizar el comando **chmod** para asignarlos. Aunque el comando **chmod** tiene formas más fáciles de leer para asignar permisos, es importante que usted comprenda el esquema de numeración puesto

que éste se utiliza en programación. Además, no todos las personas utilizan el esquema de nombrado y los usuarios de Linux a menudo suponen que si comprende los permisos de los archivos, también comprende el significado numérico.

Los grupos más comunes de tres y sus significados son los siguientes:

Permiso	Valores	Significado
---	0	Sin permiso
r--	4	Solo lectura
rw-	6	Lectura y escritura
rwx	7	Lectura, escritura y ejecución
r-x	5	Lectura y ejecución
--x	1	Sólo ejecución

A pesar de que existen otras combinaciones (por ejemplo, -wx), no son esenciales y es muy poco probable que se las encuentre.

Cada uno de estos grupos de tres letras es, posteriormente, agrupado en conjuntos de tres. El primer grupo representa los permisos para el propietario del archivo, el segundo representa los permisos para el grupo del archivo y el tercero representa los permisos para todos los usuarios del sistema. A continuación se presentan los permisos más comunes:

Permiso	Equivalente numérico	Significado
-rw-------	600	El propietario tiene permiso de lectura y escritura. Usted desea que la mayoría de sus archivos tengan estos parámetros.
-rw-r--r--	644	El propietario tiene permisos de lectura y escritura. El grupo y el mundo tiene permisos de solo lectura. Asegúrese de que permitirá a otra persona leer este archivo.
-rw-rw-rw-	666	Todos tienen permisos de lectura y escritura en un archivo. Esta configuración es mala. Usted no desea que otras personas puedan modificar sus archivos.
-rwx------	700	El propietario tiene permisos de lectura, escritura y ejecución. Usted querrá estos parámetros para programas que desea correr (como el archivo que resulta de compilar un programa en C o C++).
-rwxr-xr-x	755	El propietario tiene permisos de lectura, escritura y ejecución. El resto del mundo tiene permisos de lectura y ejecución.

Permiso	Equivalente numérico	Significado
-rwxrwxrwx	777	Todos tienen privilegios de lectura, escritura y ejecución. Como el parámetro 666, esta opción es mala. Permitir que los demás editen sus archivos es una vía segura al desastre.
-rwx--x--x	711	El propietario tiene permisos de lectura, escritura y ejecución. El resto del mundo tiene permisos de solo ejecución. Esta configuración es útil en programas que permite que otros corran pero no que copien.
drwx------	700	Éste es un directorio creado con el comando **mkdir**. Solo el propietario puede leer y escribir en él. Observe que todos los directorios deben tener el bit de ejecución habilitado.
drwxr-xr-x	755	Solo el propietario puede modificar este directorio, pero todos los demás pueden ver su contenido.
drwx--x--x	711	Este parámetro utiliza un truco para cuando usted desee permitir que un directorio sea leído por todo el mundo, pero que no quiera que pueda listar los archivos corriendo el comando **ls**. Esta configuración permite a los usuarios leer un directorio solo si conocen el filename que desean recuperar.

Administración y manipulación de archivos

Esta sección ofrece un panorama de las herramientas básicas de línea de comandos para administrar archivos y directorios. La mayor parte de este panorama debe serle familiar si ya ha utilizado una interfase de línea de comandos. En esencia, usted utiliza las mismas funciones de antes, pero con nuevos comandos.

cp: Copy Files

El comando **cp** se utiliza para copiar archivos. De la misma forma que el comando **ls**, éste tiene un gran número de opciones. Consulte la página man para encontrar detalles adicionales. Por omisión, este comando trabaja silenciosamente y despliega la información de status solo si existe una condición de error. A continuación se presentan las opciones más comunes:

Opción	Descripción
-f	Forzar copia. No solicita verificación.
-i	Copia interactiva. Antes de copiar archivos, hace que el usuario verifique que quiere copiar cada archivo.

Ejemplo: para copiar index.html en index-orig.html, teclee lo siguiente:

```
[root@ford /root]# cp index.html index-orig.html
```

Ejemplo: para copiar interactivamente todos los archivos que terminen con .html al directorio /tmp, teclee lo siguiente:

```
[root@ford /root]# cp -i *.html /tmp
```

mv: movimiento de archivos

Utilice el comando **mv** para mover archivos de un lugar a otro. Este comando también puede mover archivos entre particiones; sin embargo, debido a que este movimiento requiere que también se haga una copia real, a veces el comando **move** emplea más tiempo para ejecutar dicha acción.

A continuación se presentan las opciones más comunes de este comando:

Opción	Descripción
-f	Obliga a moverse.
-I	Se mueve interactivamente.

Ejemplo: para mover un archivo desde /usr/src/myprog/bin/* a /usr/bin, teclee lo siguiente:

```
[root@ford /root]# mv /usr/src/myprog/bin/* /usr/bin
```

Ejemplo: aunque Linux no cuenta con una herramienta explícita para el renombrado, usted puede utilizar **mv** para llevar a cabo esta tarea. Para renombrar /tmp/blah a /tmp/bleck, teclee lo siguiente:

```
[root@ford /root]# mv /tmp/bleck /tmp/blah
```

ln: enlazar archivos

El comando **ln** le permite establecer uno de dos tipos de enlaces: enlaces conectados y enlaces suaves. (Consulte la sección "Acerca de archivos y directorios" en este capítulo para encontrar información adicional). El formato general de este comando es el siguiente:

```
[root@ford /root]# ln original_file new_file
```

El comando **ln** tiene muchas opciones, la mayoría de las cuales jamás necesitará utilizar. La opción más común es **–s**, la cual crea un enlace simbólico en lugar de un enlace conectado.

Ejemplo: para crear un enlace simbólico de tal forma que /usr/bin/myadduser señale a /usr/local/bin/myadduser, usted deberá teclear lo siguiente:

```
[root@ford /root]# ln -s /usr/local/bin/myadduser /usr/bin/myadduser
```



find: encontrar un archivo

El comando **find** le permite encontrar archivos con base en una serie de criterios. Este comando, como los demás que ya hemos estudiado, ofrece un gran número de opciones sobre las que puede leer en su página man. A continuación se muestra el formato general del comando:

```
[root@ford /root]# find start_dir [options]
```

donde *start_dir* es el directorio a partir del cual debe comenzar la búsqueda. A continuación se muestra una lista de las opciones utilizadas con más frecuencia:

Opción	Descripción
-mount	No busca en otros sistemas de archivo que no sea en el que usted comenzó la búsqueda.
-atime *n*	Especifica que el archivo fue accesado al menos hace *n**24 horas.
-ctime *n*	Busca solo los archivos modificados el menos hace *n**24 horas.
-inum *n*	Busca un archivo que tenga el nodo-i *n*.
-amin *n*	Especifica que el archivo fue accesado hace *n* minutos.
-cmin *n*	Busca solo los archivos que se modificaron hace *n* minutos.
-empty	Busca archivos vacíos.
-mmin *n*	Especifica que el archivo se modificó hace *n* minutos.
-mtime *n*	Busca solo los archivos modificados hace *n**24 horas.
-nouser	Busca los archivos cuya UID no corresponda al usuario real en /etc/passwd.
-nogroup	Busca los archivos cuya GID no corresponda a un grupo real en /etc/group.
-perm *mode*	Especifica que los permisos del archivo deben ser configurados exactamente como *mode*.
-size *n*[*bck*]	Busca solo los archivos que tengan al menos n bloques/caracteres/kilobytes de longitud. Un bloque es igual a 512 bytes.
-print	Imprime los filenames que se encontraron.
-exec *cmd*\;	En cada archivo encontrado, ejecuta *cmd*. Si usted utiliza el shell bash, asegúrese de escribir a continuación de cada *cmd* el símbolo \; de otra forma, el shell se confundirá.
-name *name*	Especifica que el filename deberá ser *name*. Usted puede utilizar aquí expresiones normales.

Ejemplo: para encontrar todos los archivos en /tmp que no hayan sido accesados en siete días al menos, teclee lo siguiente:

```
[root@ford /root]# find /tmp -atime 7 -print
```

Ejemplo: para encontrar todos los archivos en /usr/src cuyos nombres sean *core* y, después, quitarlos, teclee lo siguiente:

```
[root@ford /root]# find /usr/src -name core -exec rm {} \;
```

Ejemplo: para encontrar todos los archivos en /home con la extensión .jpg que sean mayores de 100 KB, teclee lo siguiente:

```
[root@ford /root]# find /home -name "*.jpg" -size 100k
```

dd: convierta y copie un archivo

El comando **dd** lee el contenido de un archivo y lo envía a otro archivo. Lo que hace **dd** diferente de **cp** es que puede llevar a cabo conversiones rápidas en el archivo y aceptar datos de un dispositivo (como una cinta o un disco flexible). Cuando **dd** accede al dispositivo, no supone nada respecto al sistema de archivos, sino que recupera los datos en un formato muy básico. Por tanto, usted puede utilizar los datos para generar imágenes de discos, aun si el disco tiene un formato externo.

A continuación se presentan los parámetros más comunes de **dd**:

Opción	Descripción
if=*infile*	Especifica el archivo de entrada como *infile*.
of=*outfile*	Especifica el archivo de salida como *outfile*.
count=*blocks*	Especifica *blocks* como el número de bloques con los que **dd** debe operar antes de salir.
ibs=*size*	Configura el tamaño del bloque del dispositivo de entrada a un valor *size*.
obs=*size*	Configura el tamaño del bloque del dispositivo de salida a un valor *size*.
seek=*blocks*	Se salta un número de bloques *blocks* a la salida.
skip=*blocks*	Se salta un número de bloques *blocks* a la entrada.
swab	Convierte mayúsculas en minúsculas, y viceversa.

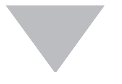
Ejemplo: para generar una imagen de un disco flexible (que es especialmente útil para formatos de archivos externos), teclee lo siguiente:

```
[root@ford /root]# dd if=/dev/fd0 of=/tmp/floppy_image
```

En las distribuciones originales de UNIX, una herramienta que comprime un archivo fue, de manera acertada, denominada **compress**. Desafortunadamente, un empresario patentó el algoritmo, esperando hacer una gran cantidad de dinero. En lugar de no hacer nada, la mayoría de los sitios vieron y descubrieron **gzip**, una herramienta diferente de compresión con un algoritmo no patentable. Aún mejor: **gzip** logra permanentemente una mejor relación de compresión que **compress**.



NOTA La herramienta **gzip** no comparte los formatos de archivo con PkZip o WinZip. Sin embargo, WinZip puede descomprimir los archivos gzip.



PISTA En general, usted puede distinguir los archivos comprimidos con **gzip** de los comprimidos con **compress** si verifica sus extensiones. Los archivos comprimidos con **gzip** típicamente terminan en .gz, mientras que los comprimidos con **compress** terminan en .Z.

A continuación, se muestran los parámetros opcionales comúnmente utilizados con **gzip**:

Opción	Descripción
-c	Escribe el archivo comprimido en el dispositivo de salida estándar.
-d	Descomprime.
-r	Recursivamente, encuentra todos los archivos que deben ser comprimidos.
-9	Proporciona la mejor compresión.
-1	Logra la compresión más rápida.

Consulte la página man para encontrar una lista completa. Observe que **gzip** comprime el archivo "en el lugar", lo que significa que después de que se efectúa la compresión, se quita el archivo original y se deja solo el archivo comprimido.

Ejemplo: para comprimir un archivo y, después, descomprimirlo, utilice el comando siguiente:

```
[root@ford /root]# gzip myfile
[root@ford /root]# gzip -d myfile.gz
```

Ejemplo: para comprimir todos los archivos que terminen en .html utilizando la mejor compresión posible, ingrese el comando siguiente:

```
[root@ford /root]# gzip -9 *.html
```

mknod: haga archivos especiales

Como ya se comentó, Linux accede a todos sus dispositivos por medio de archivos. Para crear un archivo que el sistema entienda como una interfase a un dispositivo, usted debe especificar que el archivo es del tipo bloque o carácter y que tiene un número mayor o menor. Para crear este tipo de archivo con los valores necesarios, usted puede utilizar el comando mknod.

Además de crear interfases a dispositivos, usted puede utilizar el mknod para crear tuberías nombradas.

El formato del comando es el siguiente:

```
[root@ford /root]# mknod name type [major] [minor]
```

donde *name* es el nombre del archivo y *type* es ya sea el carácter *b* para el dispositivo bloque, *c* para el dispositivo carácter o *p* para la tubería nombrada. Si usted selecciona crear un dispositivo bloque o carácter, necesita especificar el número *mayor* y el *menor*. El único momento en el que necesitará crear un dispositivo bloque o carácter es cuando instale algún tipo de controlador de dispositivo que lo requiera. La documentación que venga con su controlador deberá decirle qué valores debe utilizar para los números mayor y menor.

Ejemplo: para crear una tubería nombrada que se llame /tmp/mypipe, usted teclearía lo siguiente:

```
[root@ford /root]# mknod /tmp/mypipe p
```

mkdir: cree un directorio raíz

El comando **mkdir** en Linux es idéntico al de otras versiones de UNIX así como a las de MS-DOS. La única opción disponible es **–p**, la cual crea un directorio pariente si es que no existe ninguno. Por ejemplo, si necesita crear /tmp/bigdir/subdir/mydir y el único directorio que existe es /tmp, si utiliza **–p** automáticamente creará bigdir y subdir junto con mydir.

Ejemplo: para crear un directorio llamado mydir, teclee lo siguiente:

```
[root@ford /root]# mkdir mydir
```



NOTA En Linux, usted no puede abreviar el comando **mkdir** como **md**, como en el caso del DOS.

rmdir: quitar un directorio

El comando **rmdir** no presenta nada diferente si está familiarizado con la versión DOS del comando. Simplemente elimina un directorio existente. El único parámetro de línea de comandos disponible para este comando es **–p**, el cual elimina también los directorios pariente. Por ejemplo, si el directorio /tmp/bigdir/subdir/mydir existe y usted desea deshacerse de todos los directorios desde bigdir hasta mydir, necesitará generar solo el comando siguiente:

```
[root@ford /tmp]# rmdir -p bigdir/subdir/mydir
```

Ejemplo: para eliminar un directorio que se llame mydir, teclee lo siguiente:

```
[root@ford /root]# rmdir mydir
```



NOTA En Linux, usted no puede abreviar el comando **rmdir** como **rd** de la forma como lo hace con DOS.



pwd: despliega el directorio de trabajo actual

Es inevitable que, en un momento dado, usted se encuentre frente a una estación de trabajo que ya haya ingresado al sistema y no sepa dónde se encuentra ubicado dentro del árbol de directorios. Para obtener esta información, es necesario teclear el comando **pwd**. No tiene parámetros y su función principal es imprimir el directorio de trabajo actual. El equivalente en DOS es teclear solo **cd**; sin embargo, en bash, teclear cd simplemente lo regresa al directorio raíz.

Ejemplo: para obtener el directorio de trabajo actual, teclee el comando siguiente:

```
[root@ford src]# pwd
/usr/local/src
```

tar: archivo cinta

Si está familiarizado con el programa **pkzip**, está acostumbrado a las herramientas de compresión no solo para reducir el tamaño del archivo, sino también para combinar múltiples archivos en un archivo único de gran tamaño. Linux divide este proceso en dos herramientas. La herramienta de compresión es **gzip**.

El programa **tar** combina archivos múltiples en un archivo único de gran tamaño. La razón de separar este programa de la herramienta de compresión es que **tar** le permite seleccionar qué herramienta de compresión va a utilizar o si usted aún desea comprimir. Además, **tar** puede leer y escribir en dispositivos de manera muy similar a **dd**, lo que hace que **tar** sea una buena herramienta para respaldar dispositivos de cinta.



NOTA Aunque el nombre del programa incluye la palabra tape, no es necesario que lea o escriba en un controlador de cinta cuando cree archivos. En realidad, usted rara vez utilizará **tar** con un controlador de cinta en su trabajo cotidiano (independientemente de sus respaldos).

La estructura del comando **tar** es el siguiente:

```
[root@ford /root]# tar [commands and options] filenames
```

Los comandos y opciones disponibles de **tar** son las siguientes:

Opciones	Descripciones
-c	Crea un archivo nuevo.
-t	Presenta el contenido de un archivo.
-x	Extrae el contenido de un archivo.
-f	Especifica el nombre del archivo (o dispositivo) en el que se ubica el archivo.
-v	Sea abundante en palabras durante las operaciones.
-z	Supone que el archivo ya está (o estará) comprimido con **gzip**.

Existen muchas más opciones cuyo uso es menos frecuente. Consulte la página man para encontrar una lista más completa.

Ejemplo: para crear un archivo llamado apache.tar que contenga todos los archivos desde /usr/src/apache, teclee lo siguiente:

```
[root@ford src]# tar -cf apache.tar /usr/src/apache
```

Ejemplo: para crear un archivo llamado apache.tar que contenga todos los archivos desde /usr/src apache y vea la lista de archivos a medida que se agregan al archivo, teclee lo siguiente:

```
[root@ford src]# tar -cvf apache.tar /usr/src/apache
```

Ejemplo: para crear un archivo comprimido con gzip que se llame apache.tar.gz y que contenga todos los archivos desde /usr/src/apache y presente los fólders a medida que se van agregando al archivo, teclee lo siguiente:

```
[root@ford src]# tar -cvzf apache.tar.gz /usr/src/apache
```

Ejemplo: para extraer el contenido de un archivo tar comprimido con gzip que se llame apache.tar.gz y liste los archivos conforme se van extrayendo, teclee lo siguiente:

```
[root@ford /root]# tar -xvzf apache.tar.gz
```

cat: archivos concatenados

El programa **cat** sirve a un simple propósito: desplegar el contenido de archivos. Mientras que usted puede hacer cosas más creativas con él, casi siempre utilizará el programa simplemente para desplegar el contenido de archivos de texto, de forma muy parecida a la que utilizaría el comando **type** en DOS. Debido a que usted puede especificar nombres de archivo múltiples en la línea de comandos, es posible concatenar archivos en un único archivo más grande. Por tanto, **cat** difiere de **tar** en que el archivo resultante no cuenta con información de control para mostrar las fronteras de los diferentes archivos.

Ejemplo: para desplegar el archivo /etc/passwd, teclee lo siguiente:

```
[root@ford /root]# cat /etc/passwd
```

Ejemplo: para desplegar el archivo /etc/passwd y el archivo /etc/group, teclee lo siguiente:

```
[root@ford /root]# cat /etc/passwd /etc/group
```

Ejemplo: para concatenar el archivo /etc/passwd con el archivo /etc/group en el archivo /tmp/complete, teclee lo siguiente:

```
[root@ford /root]# cat /etc/passwd /etc/group > /tmp/complete
```

Ejemplo: para concatenar el archivo /etc/passwd a un archivo existente llamado /tmp/orb, teclee lo siguiente:

```
[root@ford /root]# cat /etc/passwd >> /tmp/orb
```

more: despliega un archivo en la pantalla a la vez

El comando more funciona de manera muy parecida a la versión DOS del programa. Despliega un archivo de entrada una pantalla a la vez. El archivo de entrada puede provenir de la entrada estándar de **more** de un parámetro de la línea de comandos.

Existen parámetros adicionales de línea de comandos para éste en particular; sin embargo, se utilizan muy de vez en cuando. Consulte la página man para encontrar información adicional.

Ejemplo: para ver el archivo /etc/passwd una pantalla a la vez, teclee lo siguiente:

```
[root@ford /root]# more /etc/passwd
```

Ejemplo: para ver la lista de directorios generados por el comando **ls** una pantalla a la vez, teclee lo siguiente:

```
[root@ford /root]# ls | more
```

du: utilización del disco

A menudo necesitará determinar dónde y quién está consumiendo espacio en disco, ¡especialmente cuando éste se encuentre corriendo muy despacio! El comando **du** le permite determinar la utilización del disco en cada directorio.

Las siguientes son algunas de las opciones del comando **du**:

Opciones	Descripción
-c	Genera un gran total al final de la corrida.
-h	Imprime los tamaños en formato legible para el ser humano.
-k	Imprime los tamaños en kilobytes en vez de hacerlo en tamaños de los bloques. (Pista: en Linux, un bloque es igual a 1 KB. Sin embargo, esto no es válido para todas las versiones de UNIX).
-s	En resumen: Imprime solo una salida para cada argumento.

Ejemplo: para desplegar en un formato legible para el ser humano la cantidad de espacio que cada directorio consume en el directorio /home, teclee lo siguiente:

```
[root@ford /root]# du -sh /home/*
```

which: despliega el directorio en el que se ubica un archivo

El comando **which** busca su trayectoria a fin de encontrar el nombre del archivo especificado en la línea de comandos. Si encuentra el nombre del archivo, la herramienta despliega la trayectoria real del archivo solicitado. El propósito de este comando es ayudarle a encontrar trayectorias totalmente calificadas.

Por ejemplo: para encontrar en qué directorio se encuentra el comando **ls**, teclee lo siguiente:

```
[root@ford /root]# which ls
```

whereis: localiza las páginas binaria, de fuente y manual de un comando

Como la descripción lo establece, este programa no sólo busca su trayectoria y despliega el nombre del programa y su directorio absoluto, sino que también busca el archivo fuente (si está disponible) y la página man del comando (de nuevo, si está disponible).

Ejemplo: para encontrar la ubicación de las páginas binaria, de fuente y manual del comando **grep**, teclee lo siguiente:

```
[root@ford /root]# whereis grep
```

df: encuentre la cantidad de espacio libre en un disco

El programa **df** despliega la cantidad de espacio libre de partición en partición. Los controladores/particiones deben montarse en **df** para recuperar esta información. Usted también puede reunir información sobre NFS mediante este comando.

A continuación se muestran algunos parámetros que usted puede utilizar con esta herramienta:

Opciones	Descripción
-h	Utilice una medición legible por los humanos, que sea diferente al número de bloques libres, para indicar la cantidad de espacio libre.
-l	Presente solo los sistemas de archivos montados que sean locales. No despliegue ninguna información acerca de los sistemas de archivos montados en la red.

Están disponibles opciones de línea de comandos adicionales; sin embargo, se utilizan muy rara vez. Usted puede conocer más acerca de ellas en la página man **df**.

Ejemplo: para mostrar el espacio libre de todos los controladores montados localmente, teclee lo siguiente:

```
[root@ford /root]# df -l
```

Ejemplo: para mostrar el espacio libre en un formato legible para el ser humano del sistema de archivos en el que está ubicado su directorio de trabajo actual, teclee lo siguiente (el punto del final es una abreviatura que significa "directorio actual", de la misma forma en que se hace en DOS):

```
[root@ford /root]# df -h .
```

Ejemplo: para mostrar el espacio libre en un formato legible para el ser humano del sistema de archivos en el que se ubica /tmp, teclee lo siguiente:

```
[root@ford /root]# df -h /tmp
```



sync: sincronización de los discos

Como lo hacen los demás sistemas operativos modernos, Linux trata de mejorar su eficiencia manteniendo un disco caché. Sin embargo, esto significa que en un momento dado no todo lo que usted desee que sea escrito en el disco lo va a estar.

Para programar que el contenido del disco caché se escriba en el disco, utilice el comando **sync**. Si **sync** detecta que la escritura del disco caché en el disco ha sido programada, esta herramienta provoca que el kernel vacíe inmediatamente el disco caché.

El comando **sync** no cuenta con parámetros de línea de comandos.

Ejemplo: para asegurar que la memoria caché del disco se haya vaciado, teclee lo siguiente:

```
[root@ford /root]# sync ;  sync
```

Manipulación del proceso

En Linux (y UNIX en general), cada programa que se corre está compuesto por al menos un proceso. Desde el punto de vista del sistema operativo, cada proceso es independiente uno del otro y, a menos de que usted les solicite que compartan los recursos entre ellos, se encuentran confinados a la memoria y ubicación en el CPU que se les asignó. Los procesos que sobrepasaron la cantidad de memoria que se les asignó (los cuales, potencialmente, pudieron corromper otro programa que estuviera corriendo y, por tanto, inestabilizar el sistema) son eliminados inmediatamente. Este método de manejar los procesos ha sido una de las razones fundamentales por la que UNIX ha podido sostener sus derechos sobre la estabilidad del sistema por tanto tiempo: las aplicaciones de los usuarios no pueden afectar a otros programas de usuario o al sistema operativo.

Esta sección estudia las herramientas utilizadas para listar y manipular procesos. Este procedimiento es muy importante para el trabajo cotidiano del administrador del sistema, puesto que es vital vigilar lo que está pasando.

ps: lista de procesos

El comando **ps** le permite listar todos los procesos de un sistema, así como su estado, su tamaño, su nombre, su propietario, su tiempo de CPU, su tiempo medido y muchas otras cosas más. El comando tiene muchos parámetros de línea, pero en esta sección se estudian solo los más comunes:

Opciones	Descripción
-a	Muestra todos los procesos con una terminal de control, no solo con la del usuario actual.
-r	Muestra solo los procesos que se llevan a cabo.
-x	Muestra los procesos que no cuentan con una terminal de control.
-u	Muestra a los propietarios de los procesos.
-f	Muestra qué procesos son parientes entre sí.
-l	Genera un formato largo.
-w	Muestra los parámetros del línea de comandos de los procesos (hasta la mitad de una línea).
-ww	Muestra todos los parámetros de línea de comandos de los procesos, sin importar su longitud.

El parámetro más común que se utiliza con el comando **ps** es **–auxww**, que muestra todos los procesos (sin considerar si tienen o no una terminal de control), los propietarios de cada proceso y todos los parámetros en línea de todos los procesos. Examinemos la salida del comando **ps –auxww**:

```
USER     PID %CPU %MEM   VSZ  RSS TTY    STAT START   TIME COMMAND
root       1  0.0  0.3  1096  476 ?      S    Jun10   0:04 init
root       2  0.0  0.0     0    0 ?      SW   Jun10   0:00 [kflushd]
root       3  0.0  0.0     0    0 ?      SW   Jun10   0:00 [kpiod]
root       4  0.0  0.0     0    0 ?      SW   Jun10   0:00 [kswapd]
root       5  0.0  0.0     0    0 ?      SW<  Jun10   0:00 [mdrecoveryd]
root     102  0.0  0.2  1068  380 ?      S    Jun10   0:00 /usr/sbin/apmd -p 10 -w 5
bin      253  0.0  0.2  1088  288 ?      S    Jun10   0:00 portmap
root     300  0.0  0.4  1272  548 ?      S    Jun10   0:00 syslogd -m 0
root     311  0.0  0.5  1376  668 ?      S    Jun10   0:00 klogd
daemon   325  0.0  0.2  1112  284 ?      S    Jun10   0:00 /usr/sbin/atd
root     339  0.0  0.4  1284  532 ?      S    Jun10   0:00 crond
root     357  0.0  0.3  1232  508 ?      S    Jun10   0:00 inetd
root     371  0.0  1.1  2528 1424 ?      S    Jun10   0:00 named
root     385  0.0  0.4  1284  516 ?      S    Jun10   0:00 lpd
root     399  0.0  0.8  2384 1116 ?      S    Jun10   0:00 httpd
xfs      429  0.0  0.7  1988  908 ?      S    Jun10   0:00 xfs
root     467  0.0  0.2  1060  384 tty2   S    Jun10   0:00 /sbin/mingetty tty2
root     468  0.0  0.2  1060  384 tty3   S    Jun10   0:00 /sbin/mingetty tty3
root     469  0.0  0.2  1060  384 tty4   S    Jun10   0:00 /sbin/mingetty tty4
root     470  0.0  0.2  1060  384 tty5   S    Jun10   0:00 /sbin/mingetty tty5
root     471  0.0  0.2  1060  384 tty6   S    Jun10   0:00 /sbin/mingetty tty6
root     473  0.0  0.0  1052  116 ?      S    Jun10   0:01 update (bdflush)
root     853  0.0  0.7  1708  940 pts/1  S    Jun10   0:00 bash
root    1199  0.0  0.7  1940 1012 pts/2  S    Jun10   0:00 su
root    1203  0.0  0.7  1700  920 pts/2  S    Jun10   0:00 bash
root    1726  0.0  1.3  2824 1760 ?      S    Jun10   0:00 xterm
root    1728  0.0  0.7  1716  940 pts/8  S    Jun10   0:00 bash
root    1953  0.0  1.3  2832 1780 ?      S    Jun11   0:05 xterm
root    1955  0.0  0.7  1724  972 pts/10 S    Jun11   0:00 bash
nobody 6436  0.0  0.7  2572  988 ?      S    Jun13   0:00 httpd
nobody 6437  0.0  0.7  2560  972 ?      S    Jun13   0:00 httpd
nobody 6438  0.0  0.7  2560  976 ?      S    Jun13   0:00 httpd
nobody 6439  0.0  0.7  2560  976 ?      S    Jun13   0:00 httpd
nobody 6440  0.0  0.7  2560  976 ?      S    Jun13   0:00 httpd
nobody 6441  0.0  0.7  2560  976 ?      S    Jun13   0:00 httpd
root   16673  0.0  0.6  1936  840 pts/10 S    Jun14   0:00 su -sshah
sshah  16675  0.0  0.8  1960 1112 pts/10 S    Jun14   0:00 -tcsh
root   18243  0.0  0.9  2144 1216 tty1   S    Jun14   0:00 login -- sshah
sshah  18244  0.0  0.8  1940 1080 tty1   S    Jun14   0:00 -tcsh
```



La primera línea de la salida es el encabezado, que indica el significado de cada columna. La mayoría se explican por sí mismos:

Encabezado	Descripción
USER	Nombre de usuario del propietario de cada proceso.
PID	Número de identificación del proceso.
%CPU	Porcentaje de CPU que consume el proceso. ¡Recuerde que para un sistema con procesadores múltiples, esta columna crecerá más de 100%!
%MEM	Porcentaje de memoria que consume un proceso.
VSZ	Cantidad de memoria virtual que toma un proceso.
RSS	Cantidad de memoria real (residente) que toma un proceso.
TTY	Terminal de control de un proceso. Un signo de interrogación (?) significa que el proceso ya no se encuentra conectado a la terminal de control.
STAT	Estado del proceso. S significa que el proceso está dormido. Recuerde que todos los procesos que estén listos para correrse (esto es, los procesos que se asignaron como multitarea mientras que el CPU está momentáneamente enfocado en otros procesos) estarán dormidos. R significa que, en realidad, el proceso se encuentra en el CPU y D es un estado ininterrumpible de sueño (generalmente relacionado con I/O). T significa que el proceso está siendo rastreado por un depurador o ha sido detenido. Z significa que el proceso actúa como un zombie. "Actuar como zombie" significa una de estas dos situaciones: que el proceso pariente no haya reconocido la muerte de su hijo utilizando la llamada de espera del sistema, o que el pariente fue muerto inadecuadamente y, por tanto, el proceso de inicio no puede sacar provecho del hijo hasta que el pariente esté completamente muerto. Por lo general, un proceso zombie indica un software pobremente escrito. Cada estado del proceso puede tener un modificador como sufijo. Dentro de estos modificadores están incluidos W, <, N y L. W significa que el proceso no tiene páginas residentes en memoria (ha sido totalmente borrado), < indica que se trata de un proceso con alta prioridad, N indica una tarea con baja prioridad y, por último, L comunica que algunas páginas están encerradas en la memoria (lo cual generalmente significa la necesidad de una funcionalidad en tiempo real).
START	Fecha en la que se inició el proceso.
TIME	Cantidad de tiempo que el proceso ha pasado en el CPU.
COMMAND	Nombre el proceso y sus parámetros de línea de comandos.

top: muestra una lista de procesos interactiva

El comando **top** es una versión interactiva de **ps**. En lugar de proporcionar una vista interactiva de lo que está pasando, esta herramienta refresca la pantalla con una lista de procesos cada dos o tres segundos (el usuario puede ajustar el intervalo). En esta lista, usted puede volver a establecer prioridades o matar procesos.

La cuestión fundamental con el programa **top** es que representa un problema para el CPU. En un sistema congestionado, este problema tiende a empeorar las dificultades con la memoria a medida que los usuarios comienzan a correr el comando **top** para ver qué está pasando, solo para ver que las demás personas también lo están utilizando y ¡que todos, colectivamente, han hecho que el sistema trabaje más lentamente que antes!

Por omisión, el comando top se instala con permisos otorgados a todos los usuarios. Usted puede considerar prudente, dependiendo de su ambiente, permitir que solo el directorio raíz pueda correrlo. Para ello, cambie el permiso del programa **top** con el comando siguiente:

```
[root@ford /root]# chmod 0700 /usr/bin/top
```

kill: envía una señal a un proceso

Por alguna razón, el programa kill tiene un nombre horrible: ¡En realidad, el programa no mata procesos! Lo que hace es enviar señales a los procesos que se encuentran corriendo. El sistema operativo, por omisión, proporciona a cada proceso un conjunto estándar de *manejadores de señal* para que atiendan a las señales entrantes. Desde el punto de vista del administrador de sistemas, el manejador más importante es el de los números de señales de 9 al 15: el proceso matar y el proceso terminar. (De acuerdo, quizás utilizar *kill* como nombre no fue inapropiado, después de todo…).

Cuando se invoca el comando **kill**, se requiere al menos un parámetro: el número de identificación del proceso (PID) como se dedujo a partir del comando **ps**. Cuando se transfiere solo el número PID, **kill**, por omisión, enviará la señal 15, y termina el proceso. El envío de la señal de terminar el proceso es muy similar a solicitar amablemente que un proceso deje de hacer lo que está haciendo y se apague. Algunos programas interceptan esta señal y efectúan un número de acciones de forma que puedan apagarse de manera normal. Otros, solo se detienen repentinamente. De cualquier forma, el envío de la señal no es un método garantizado para detener un proceso.

El parámetro opcional es un número prefijado por una carácter guión (-), en cuyo caso el número representa un número de señal. Las dos señales en las que los administradores de sistemas están más interesados son el 9 y el 1: elimina y mantente en espera. La señal kill es la forma poco amable de hacer que un proceso se detenga. En lugar de solicitar al proceso que se detenga, el sistema operativo mata al proceso. La única forma en la que esta señal falla es cuando el proceso se encuentra a la mitad de una llamada de sistema (como una solicitud de abrir un archivo), en cuyo caso el proceso morirá una vez que regrese de la llamada del sistema.

La señal mantente en espera es un poco de retroceso cuando la mayoría de los usuarios de UNIX se conectan al sistema a través de terminales tipo VT-100. Cuando una conexión de usuario deja de funcionar a la mitad de una sesión, todo su proceso que está corriendo recibirá la señal de

mantenerse en espera (a menudo un SIGHUP o HUP abreviado). Esta señal le ofrece al proceso la oportunidad de llevar a cabo un apagado normal o, en el caso de algunos programas diseñados para mantenerse corriendo tras bambalinas, ignorar la señal.

En estos días, la señal HUP se utiliza para informar a ciertas aplicaciones de servidor que vuelvan a leer sus archivos de configuración. De otra forma, la mayoría de las aplicaciones ignora la señal.

Aspectos de seguridad de kill La capacidad para terminar un proceso es, evidentemente, la más poderosa. Los desarrolladores del comando **kill** se percataron de ello y se aseguraron de que se tomaran medidas de seguridad, de forma que los usuarios pudieran matar solo aquellos procesos que tuvieran permiso de hacerlo. Por ejemplo, los usuarios no raíz podrían enviar señales solo a sus propios procesos. Si un usuario no raíz intenta enviar señales a procesos que no le pertenecen, el sistema genera mensajes de error. Por otro lado, puede enviar señales a todos los procesos del sistema. Ello significa, por supuesto, que cuando se utilice el comando **kill**, el usuario raíz necesita ser extremadamente cuidadoso a fin de asegurarse de que el usuario ¡no mate accidentalmente al proceso equivocado!

Ejemplo: para eliminar el proceso 2059, teclee lo siguiente:

```
[root@ford /root]# kill 2059
```

Ejemplo: para matar el proceso número 593 de forma casi garantizada, teclee lo siguiente:

```
[root@ford /root]# kill -9 593
```

Ejemplo: para enviar el programa init (que es siempre el proceso ID 1) a la señal HUP, teclee lo siguiente:

```
[root@ford /root]# kill -1 1
```

Herramientas misceláneas

Si este libro estuviera dedicado completamente a estudiar los comandos disponibles en su sistema Linux, cada una de las herramientas que se analizan en esta sección caería en varias categorías que serían más específicas. Sin embargo, puesto que este panorama se enfoca solamente en las herramientas más importantes para llevar a cabo las tareas administrativas cotidianas, las herramientas siguientes tendrán que categorizarse como misceláneas. Sin embargo, a pesar de que esta sección no está de acuerdo en clasificarlas bajo sus propias categorías específicas, ¡eso no significa que las herramientas no sean importantes!

uname: muestra el nombre del sistema

El programa **uname** le permite aprender algunos detalles acerca de un sistema. A menudo, esta herramienta es muy útil cuando ha logrado ingresar, de manera remota, a una docena de computadoras diferentes y no sabe dónde está. Esta herramienta también es muy útil para los escritores de scripts, ya que les permite modificar la trayectoria de un script con base en la información del sistema.

Los parámetros de línea de comandos de **uname** son los siguientes:

Opciones	Descripción
-m	Imprime el tipo de hardware de la máquina (por ejemplo, i868 para Pentium Pro y arquitecturas mejores).
-n	Imprime el nombre del host de la máquina.
-r	Imprime el nombre de la versión del sistema operativo.
-s	Imprime el nombre del sistema operativo.
-v	Imprime la versión del sistema operativo.
-a	Imprime toda la información anterior.

Podría parecer extraño que **uname** imprimiera cosas como el nombre del sistema operativo cuando el usuario evidentemente debe saber que el nombre es Linux. Sin embargo, dicha información es, en realidad, muy útil ya que usted puede toparse con el comando **uname** en casi todos los sistemas operativos tipo UNIX. Por tanto, si se encuentra en una estación de trabajo SGI y teclea **uname –s**, la herramienta le regresará IRIX; si ingresa el comando en una estación de trabajo Sun, regresará SunOS, y así sucesivamente. A menudo, las personas que trabajan en ambientes heterogéneos creen que es útil escribir sus scripts de forma que se comporten de manera diferente dependiendo del tipo de sistema operativo, y uname proporciona una forma maravillosamente congruente de determinar esa información.

Ejemplo: para obtener el nombre de un sistema operativo y su versión, teclee lo siguiente:

```
[root@ford /root]# uname -s -r
```

who: investigue quién está en el sistema

Cuando administre sistemas que le permitan a las personas ingresar a ellos por medio de máquinas ajenas o especialmente configurar servidores, usted querrá saber quién está dentro del sistema. Para generar un reporte que muestre los usuarios que se encuentran en ese momento firmados en el sistema, puede utilizar el comando **who**. Simplemente teclee lo siguiente:

```
[root@ford]# who
```

Este comando generará un reporte similar al siguiente:

```
sshah    tty1     Jun 14 18:22
root     pts/9    Jun 14 18:29 (:0)
root     pts/11   Jun 14 21:12 (:0)
root     pts/12   Jun 14 23:38 (:0)
```

su: cambie de usuarios

Una vez que se ha firmado en el sistema como un usuario, no necesita salir de él y, después, volver a ingresar bajo otra identidad (por ejemplo, si ingresó al sistema como usted mismo y desea convertirse en el usuario raíz). Simplemente utilice el comando **su** para cambiarse a otro usuario. Este comando tiene solo dos parámetros de línea de comandos, y ambos son opcionales.

Por omisión, correr el comando su sin parámetros se considera como un intento de convertirse en el usuario raíz. Linux le solicitará la contraseña de usuario; si ingresa la contraseña correcta, Linux lo llevará a un shell raíz. Si es el usuario raíz y desea tomar la identidad de otro usuario, no necesita ingresar esa contraseña.

Ejemplo: si se encuentra firmado como usted mismo y desea cambiar a usuario raíz, teclee lo siguiente:

```
[sshah@ford ~]$ su
```

Ejemplo: si se encuentra firmado como raíz y desea cambiarse a usuario sshah, teclee lo siguiente:

```
[root@ford /root]# su sshah
```

Usted puede utilizar el guión (-) como parámetro opcional. Este carácter le dice a **su** que no sólo cambie identidades, sino que también corra los scripts login para ese usuario.

Ejemplo: si está firmado como raíz y desea cambiar al usuario sshah con todas sus configuraciones de login y shell, teclee lo siguiente:

```
[root@ford /root]# su - sshah
```

RESUMEN DEL CAPÍTULO

En este capítulo se analizaron dos métodos básicos de administración de sistemas y se presentaron los cimientos para aprender más cerca de este tema. Usted aprendió acerca de la configuración de algunos de los parámetros clave del servidor utilizando las herramientas básicas integradas que tiene el sistema operativo Red Hat Linux ES. En la segunda mitad del capítulo, usted aprendió mucho más acerca de la línea de comandos de Linux y cómo controlar el sistema que lo usa.

En el capítulo, he tenido (obviamente) qué omitir información. Después de todo, la mayoría de los libros sobre administración de sistemas tiene cientos de páginas, y este capítulo no tiene ni siquiera cincuenta páginas. Sin embargo, dado todo lo que ha aprendido aquí, usted debe ser capaz de llevar a cabo tareas administrativas básicas y arreglárselas con este sistema operativo.

La forma más fácil de obtener más información es invertir tiempo para practicar con las herramientas de la línea de comandos y los diferentes programas System Tools. Las herramientas gráficas son mucho más capaces de lo que se presentó aquí. ¡En realidad, en servidores sencillos, es completamente posible llevar a cabo el mantenimiento del sistema solo mediante las herramientas gráficas! La línea de comandos, por otro lado, es el arma secreta de Linux para obtener mayor flexibilidad.

Un comentario final si desea aprender más acerca de la administración de sistemas Linux: asegúrese de consultar la referencia *Linux Administration: A Beginner´s Guide*, Fourth Edition, de Wale Soyinka (McGraw-Hill/Osborne, 2006).



CAPÍTULO 24

Configuración de un servidor web Linux con Apache

Una de las aplicaciones de servidor web más populares es el Apache, un programa sin costo que corre con una gran variedad de sistemas operativos, entre ellos Linux, Windows, OS/2, Mac OS X, Solaris y Netware. El servidor web Apache, a pesar de ser un programa sin costo de fuente abierta, es una plataforma robusta y probada en la cual se puede almacenar un sitio web. El hecho de que esté disponible sin costo, corriendo en un sistema operativo similar a UNIX que es Linux (que a menudo se encuentra disponible sin costo), es una ventaja adicional enorme que sin duda ayuda a aumentar su gran popularidad.

Este capítulo analiza el servidor web Apache y explica los fundamentos que necesita para entenderlo, bajarlo de la red, encontrar recursos basados en la web para brindarle soporte y configurar un sitio web básico en un servidor Red Hat Linux ES.

PANORAMA DEL SERVIDOR APACHE

El servidor Apache comenzó como un pequeño desarrollo en el National Center for Supercomputing Applications (NCSA) a principios de la última década del siglo pasado. Comenzó como un daemon de UNIX muy simple, inicialmente programado por Rob McCool. Éste dejó NCSA en 1994, y el proyecto comenzó a crecer debido al empuje de un gran número de programadores, algunos de los cuales le agregaron paquetes (módulos) al programa principal para habilitarlo como soporte de nuevas tecnologías web. En aquellos días, al servidor web se le conocía como servidor "parchado", debido a que continuamente se le agregaban nuevos parches para corregir problemas o extender su funcionalidad. Finalmente, se le comenzó a llamar servidor web Apache.

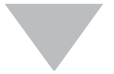
La versión 1.0 de este servidor se liberó al público a finales de 1995, y para 1996 era el más popular en internet. Las últimas estadísticas, hasta el momento en que se escribió este capítulo, que datan de marzo del 2005 (**http://news.netcraft.com/archives/web_server_survey.html**), revelan que Apache actualmente sirve como host a aproximadamente 70% (más de 41 millones de sitios web) de los sitios web activos en Internet, mientras que el IIS de Microsoft ocupa el segundo lugar con 20% (más de 12 millones de sitios).

En la actualidad, Apache es coordinado mediante una organización llamada Apache Software Foundation, una corporación sin fines de lucro formada en 1999. Su página en Internet se localiza en **http://www.apache.org**.

Apache es diferente a la mayoría de las aplicaciones de servidor porque no es un programa gráfico (a pesar de que su propósito principal es ofrecer servicio a las páginas gráficas de la web) y no cuenta con una rutina de instalación gráfica. En lugar de eso, corre como un proceso tras bambalinas en el sistema operativo en el cual está instalado. Este proceso tras bambalinas, llamado deamon (que se pronuncia como "demon"), se llama típicamente httpd (hypertext transfer protocol deamon). La administración de un servidor Apache se maneja mediante la edición de sus archivos de configuración basados en texto, que detiene y arranca el deamon para provocar que surta efecto cualquier cambio en los archivos de configuración.

Los principiantes en el tema de la conectividad de redes probablemente estén acostumbrados a manejar todo en un servidor por medio de un tipo de interfase gráfica. Mientras que este procedimiento hace más fácil la administración de un servidor, el hecho de que Apache esté basado

en texto y sea administrado por medio de una interfase de línea de comandos no debe sorprenderle. El proceso para instalar y administrar un servidor Apache es muy directo y usted no deberá tener problemas para llevarlo a cabo. En realidad, si siguió el procedimiento de instalación de Red Hat Linux ES del capítulo 22, entonces ya tiene instalado Apache en esa computadora; lo único que tiene que hacer es activarlo. (No está activado por omisión en una instalación Red Hat Linux ES).



NOTA Este libro está diseñado para familiarizarlo con los conceptos importantes del software y el hardware de la conectividad de redes. Usted puede pensar en este libro como una "parte medular" para aprender acerca del extenso campo de la conectividad. A partir de esta parte medular, podrá desarrollar algunos temas con mayor detalle, como la configuración y administración de servidores web Apache. Sin embargo, ahondar en estos temas va más allá del alcance de este libro.

INSTALACIÓN DEL WEB SERVER APACHE

Esta sección le muestra cómo puede configurar un sitio web utilizando el servidor web Apache bajo Red Hat Linux ES.

La forma más fácil de instalar un servidor Apache bajo Red Hat Linux es llevar a cabo la instalación por omisión. Sin embargo, si por alguna razón no instaló Apache bajo Linux (por ejemplo, si usted utiliza una distribución diferente de Linux que no venga con Apache o instaló Red Hat Linux en una estación de trabajo), puede bajar la última versión e instalarla manualmente.

Para bajar la última versión de Apache, utilice un navegador de la web para ir a **http://www.apache.org/dist/httpd/**. Abra el fólder Binaries, después el que representa el sistema operativo que está utilizando (Linux) y, por último, seleccione el paquete apropiado de la lista que aparece. Los paquetes están organizados por versión de Apache (la cual también se muestra como parte de los nombres de archivo), por procesador y por sistema operativo. Por ejemplo, puede bajar un archivo llamado httpd-2.0.39-i686-pc-linux-gnu.tar.gz (que representa la versión 2.0.39 de Apache para sistemas Pentium IV corriendo en Linux) a un directorio temporal en su sistema Linux, desde el cual podrá instalar el servidor Apache y, después, ponerlo en funcionamiento y probarlo, como se indica en los pasos siguientes:

1. Abra una ventana de emulación de terminal.
2. Para cambiarse al directorio que contiene el archivo binario de Apache que bajó, teclee **cd/*directory*** y presione ENTER.
3. Descomprima el archivo gz utilizando el comando siguiente (sustituye el nombre real del archivo que usted bajó después de "gunzip"):

```
gunzip filename.tar.gz
```

4. Desintegre el archivo resultante .tar con el comando siguiente (que sustituye el nombre del archivo real que se encuentra en el directorio después de llevar a cabo el comando gunzip en el paso 3). Usted puede utilizar el comando **ls** para ver su nombre:

   ```
   tar -xvf filename.tar
   ```

5. En el paso 4, el comando **tar** crea un directorio que tiene el mismo nombre que la porción del nombre y la versión del archivo tar. Usted deberá cambiarse a ese directorio (**cd**), de la manera siguiente:

   ```
   cd /httpd—2.0.39
   ```

6. Ahora puede correr el script de configuración de Apache. Ingrese el comando siguiente (le tomará solamente unos cuantos segundos correrlo):

   ```
   ./configure
   ```

7. Ahora prepare los binarios y compílelos. Este proceso implica dos comandos, cada uno puede tomar varios minutos en completarse:

   ```
   make
   make install
   ```

8. En este punto, Apache está instalado pero todavía no corre. Para iniciar Apache, ejecute el comando siguiente desde cualquier directorio:

   ```
   /usr/local/apache/bin/apachectl start
   ```

   Si usted está comenzando la versión de Apache que fue instalada por omisión con el Red Hat Linux ES, en lugar de lo anterior, teclee el comando siguiente:

   ```
   /usr/sbin/apachectl start
   ```

Existe un gran número de formas mediante las cuales puede probar su instalación de Apache. Primero, puede utilizar el comando **ps** para verificar que los daemons estén corriendo:

```
ps -e |more
```

El comando **ps** desplegará todos los comandos que se estén ejecutando en ese momento. Debido a que el comando anterior dirige la salida de **ps –e** a través del comando **more**, usted tendrá que presionar SPACE varias veces para ver todos los procesos que corren en ese momento. En la salida, usted deberá ver una o más copias de un proceso llamado httpd, el cual es el deamon de Apache. Usted podrá ver muchos de ellos, pues Apache generalmente activa a varios, lo cual depende de la computadora en la que lo tenga instalado, lo que es algo perfectamente normal.

Después de que haya verificado que Apache arrancó, puede también probarlo mediante el empleo de un navegador web como Netscape. Ingrese cualquiera de las direcciones web siguientes:

```
ttp://127.0.0.1
http://localhost
```

Ambos comandos accesan a cualquier servidor web que se encuentre activo en la computadora en la que se están utilizando. (Recuerde que la dirección 127.0.0.1 es siempre un equivalente de la computadora local, como es el nombre localhost). Apache tiene una página web por omisión que se instala automáticamente, la cual debe desplegarse en Netscape, como se muestra en al figura 24-1.

Usted también podrá acceder a la página desde otra computadora. Si la computadora en la que instaló Apache tiene la dirección IP 209.200.155.49, la siguiente dirección web deberá mostrar la página:

```
http://209.200.155.49
```

Si no puede acceder a la página desde una computadora remota, pero sí puede hacerlo desde la computadora local, debe verificar la conectividad básica IP mediante el comando **ping** y las técnicas típicas para la reparación de redes.

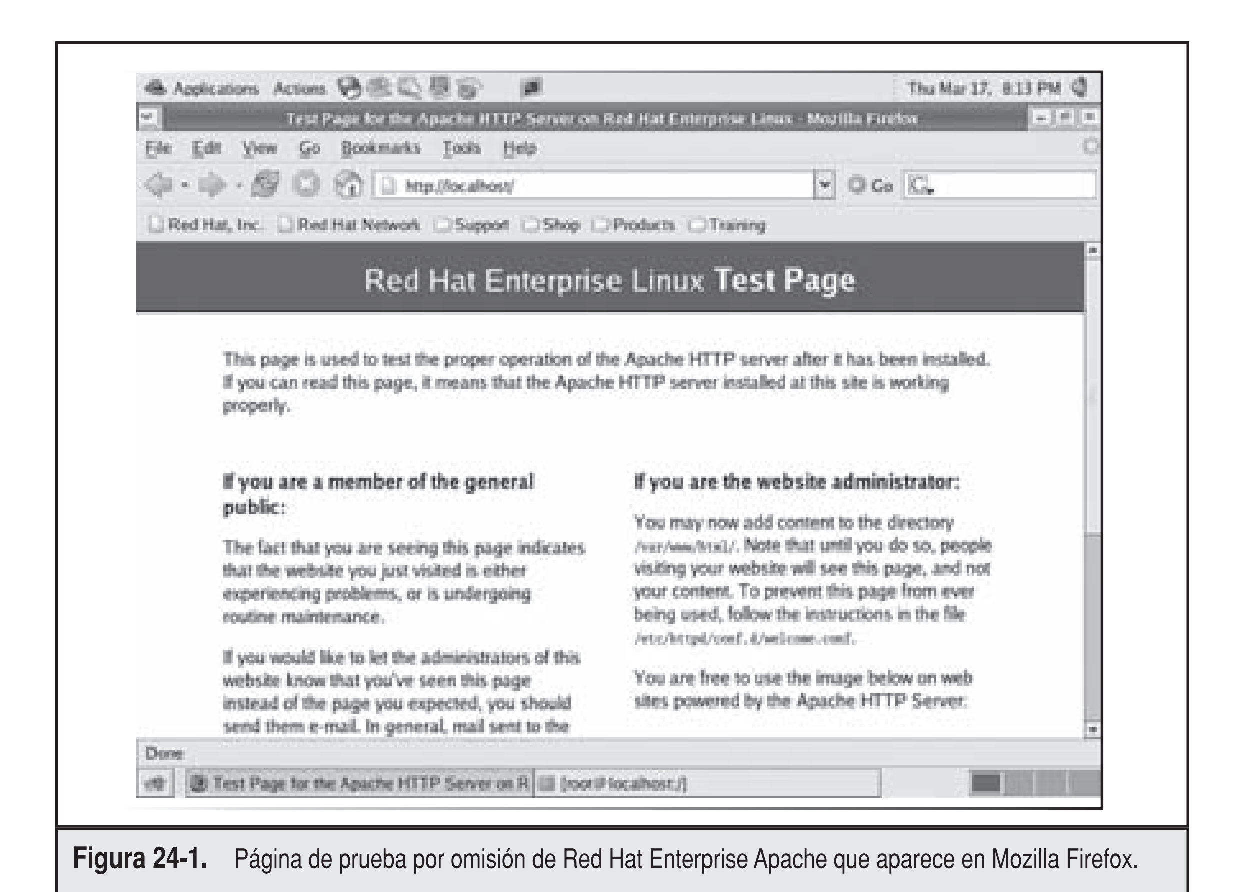


Figura 24-1. Página de prueba por omisión de Red Hat Enterprise Apache que aparece en Mozilla Firefox.

ADMINISTRACIÓN DE UN SERVIDOR WEB APACHE

Existe un gran número de tareas administrativas básicas que usted necesitará llevar a cabo en un servidor Apache. La publicación de un sitio web en su servidor recién instalado es de las de mayor importancia. Esta sección describe las tareas administrativas básicas.

Detención y arranque de Apache

Como pudo observar en el proyecto que instaló Apache en Red Hat Linux, usted utiliza un archivo script llamado apachectl para comenzar y detener el servidor. En el caso de una instalación de Red Hat Linux ES por omisión, el archivo apachectl está ubicado en el directorio /usr/sbin y tiene tres parámetros importantes: comenzar, detener y reiniciar. Por ejemplo, el comando siguiente reiniciará el servidor:

```
/usr/sbin/apachectl restart
```

Cambio de la configuración de Apache

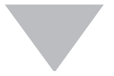
Como se mencionó antes, Apache está básicamente controlado por medio de archivos de configuración basados en texto, el más importante de los cuales es httpd.conf. Este archivo se localiza en el directorio siguiente:

```
/etc/httpd/conf/
```

El archivo httpd.conf trabaja por medio del uso de directivas en texto normal contenido en el archivo, junto con los parámetros asociados. Por ejemplo, la directiva siguiente define dónde está instalado Apache:

```
ServerRoot "/etc/httpd"
```

Si usted quisiera transferir una instalación Apache a un directorio diferente en su computadora Linux podría hacerlo, pero deberá ser muy cuidadoso al cambiar la configuración del ServerRoot antes de intentar reiniciar Apache en su nueva ubicación.



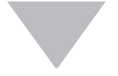
NOTA Para que los cambios en el archivo httpd.conf tengan efecto, usted debe reiniciar Apache mediante el comando **./apachectl restart**.

El archivo httpd.conf se divide en tres secciones principales, de la manera siguiente:

- Ambiente global
- Configuración del servidor principal
- Hosts virtuales

Cada sección contiene un gran número de directivas que controlan la forma en que trabaja Apache.

En el proceso de aprendizaje de Apache, es recomendable invertir cierto tiempo en el estudio del contenido del archivo httpd.conf y en la lectura de los exhaustivos comentarios que están incluidos en el archivo. Usted también deberá consultar las diferentes directivas en la documentación en línea de Apache, ya que los comentarios incluidos en el archivo httpd.conf no deben considerarse completamente informativos.

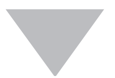


NOTA La documentación en línea de Apache está instalada localmente en sistemas Red Hat Linux ES en el directorio /var/www/manual. Una vez que Apache se encuentre activo y en operación, usted podrá verlo con un navegador web utilizando la dirección **http://localhost/manual/index.html,** pero también podrá accesarlo en **http://www.apache.org**.

Publicación de páginas web

Por omisión (en la versión 2 de Apache), el sitio web principal publicado por Apache se encuentra en el directorio /var/www/html. También por omisión, este directorio está vacío.

Una vez que usted esté listo para publicar un sitio web completo, podrá colocar los archivos en /var/www/html en la página de inicio almacenada como index.html. La forma más fácil de hacerlo es conectándose a la computadora que corre Apache mediante el empleo del programa ftp, para después subir los archivos del sitio web, ya sea directamente al directorio /var/www/html o a un directorio temporal en el disco duro del servidor. Una vez que se encuentren en el directorio temporal, usted podrá moverlos a la ubicación correcta en el mismo servidor mediante los comandos **mv** o **cp**.



NOTA El capítulo 23 abarca un gran número de comando de Linux/UNIX de gran utilidad, como **mv** y **cp**.

RESUMEN DEL CAPÍTULO

En el transcurso de su vida será necesario que la mayoría de los profesionales en conectividad de redes instale y proporcione mantenimiento a un servidor web. Todas las plataformas de servidor cuentan con servidores web que están disponibles para dichos profesionales. Un servidor excelente que se encuentra disponible para casi todas las plataformas es el servidor web Apache. Como pudo ver en este capítulo, es fácil de instalar, administrar y hacer que trabaje. Si usted ha seguido las instrucciones de este libro y ha instalado y utilizado Red Hat Linux ES en un sistema de prueba, recomiendo que también siga los pasos que se indican en este capítulo e instale y ponga a funcionar a Apache, aun mediante la adición de algunos archivos para un simple sitio web en él y navegue en el servidor web, primero desde la computadora en la que está corriendo y, después, desde cualquier otra computadora de la red.



GLOSARIO

10Base-2 Especificación a 10 Mbps (bandabase) transportada a través de cable coaxial. También se le conoce como Thin Ethernet o Thinnet.

10Base-5 Especificación a 10 Mbps (bandabase) transportada a través de cable coaxial delgado. También se le conoce como Thick Ethernet o Thicknet.

10Base-Fx Especificación a 10 Mbps (bandabase) transportada a través de fibra óptica.

10Base-T Especificación a 10 Mbps (bandabase) transportada a través de cable de par trenzado.

100Base-Tx Especificación a 100 Mbps (bandabase) transportada a través de cable de par trenzado.

1 000Base-T Especificación a 1000 Mbps (un gigabit) transportada a través de cable de par trenzado.

802.x Especificación para diferentes tipos de redes Ethernet.

AAUI Unidad de Interfase de Conexión de Apple. Conector para enlazar una Macintosh a una red Ethernet.

Administrador Gerente general de una red. Por lo general, tiene permiso de llevar a cabo cualquier tarea en una red, de acceder a cualquier recurso y puede asignar derechos a los usuarios de la red. A menudo se le conoce como *supervisor* o *superusuario.*

AFP Protocolo de archivo de Apple. Protocolo de acceso al archivo para trabajar con archivos a través de una red.

Analógico Señal eléctrica que tiene múltiples estados y que, en general, tiene un número infinito de valores. Por ejemplo, una perilla de radio es, en general, un ajuste analógico.

Ancho de banda Cantidad de datos que pueden transportarse a través de una red que, generalmente, se expresa en mega (millones) de bits por segundo o Mbps. A veces, el ancho de banda también se especifica en Hertz, como en el caso de 10 megahertz (MHz).

ANSI Instituto Nacional de Estándares Estadounidenses. Organización privada, no lucrativa que coordina los estándares en Estados Unidos.

AppleTalk Grupo de protocolos sobre conectividad de redes para computadoras Macintosh.

ARCnet Protocolo de red de estafeta circulante que, en la actualidad, se utiliza muy rara vez.

ATM Modo de transferencia asíncrono. Especificación de red conmutada y multiplexada a alta velocidad.

Atributos (archivo) Características que se les dan a los archivos. Por ejemplo, en los archivos DOS, dentro de los atributos se incluyen Solo lectura, Sistema oculto y Archivo. Los sistemas de red, en general, agregan dichos atributos como Compartible o Inhibir la eliminación.

AUI Unidad de interfase de conexión. Caja que conecta un cable de red a un transceptor.

Banda ancha Cable de red que puede transportar múltiples señales de forma simultánea. Vea Bandabase.

Bandabase Cable de red que puede transportar solamente una señal a la vez. Véase *Banda ancha*.

Bit Abreviatura de *dígito binario*, esto es, un solo dígito que tiene un valor 0 ó 1.

Bit de archivo Bit que indica qué archivos necesitan archivarse (respaldarse). Cuando se realiza un respaldo, el bit de archivo se pone en ceros. Cualquier cambio subsecuente al archivo provoca que el bit se ponga en uno, lo cual indica la necesidad de un archivo.

Buffer Memoria independiente de los datos caché entre dos dispositivos que proporciona acceso más rápido a los datos que se utilizan con mayor frecuencia. A menudo, los sistemas operativos utilizan buffers para guardar los datos usados con frecuencia que están almacenados en discos.

Bus 1) Topología de red en la que el cable corre de un nodo a otro, con un terminador en cada extremo. 2) Espina dorsal de las conexiones utilizadas en una computadora. La mayoría de los periféricos se conectan a ella.

Bus ISA Bus de la Arquitectura de Estándares Industriales. Bus de computadora originalmente desarrollado para la IBM PC-AT.

Bus MCA Bus con arquitectura de micro-canal. Estándar de bus de computadora elaborado por IBM que no fue aceptado ampliamente.

Byte Colección de 8 bits que puede representarse con hasta 256 valores diferentes.

Cable coaxial Cable con un conductor en su centro y envuelto por una protección. Los tipos más comunes de cable coaxial son RG-58 y RG-8.

Cable de conexiones Cable que permite la conexión de dos tipos de equipos de comunicaciones que, normalmente, no se comunican directamente entre sí. Por ejemplo, el equipo de comunicación de datos se clasifica como equipo terminal de datos (DTE) o equipo de comunicación de datos (DCE). Por lo general, el equipo DTE puede comunicarse sólo con equipo DCE. Un cable de conexiones permite que dos equipos DTE o dos DCE se comuniquen.

Caché Memoria independiente que se utiliza expresamente para almacenar datos que se acceden con mucha frecuencia desde un disco.

Canal-B Canal de una conexión ISDN que transporta (normalmente) 64 Kbps de datos.

Canal-D Uno de los canales utilizados en todas las interfases ISDN; transporta 16 Kbps de datos y se utiliza para establecer la llamada y otras tareas de control de señales. A pesar de que también se le llama *canal de datos*, en realidad no transporta datos del usuario.

Capa de aplicación Séptima capa y la más alta del modelo OSI de conectividad de redes. Maneja las comunicaciones entre las aplicaciones a través de la red. A menudo, lleva a cabo la autentificación del usuario en las redes.

Capa de enlace de datos Segunda capa del modelo OSI de redes que maneja las conexiones libres de errores entre dos dispositivos a través de una conexión física común.

Captura Mecanismo que habilita a una impresora de red para actuar como impresora local de una computadora específica. La salida que se envía al puerto de impresión de la computadora es "capturada" y redirigida a una impresora de red.

Central telefónica (CO) Facilidad de conmutación que es administrada por la Compañía Telefónica Regional Bell (RBOC), que proporciona un punto de acceso a la red de la RBOC.

Cinta abierta lineal (LTO) Estándar de respaldo de red creado originalmente por un consorcio industrial formado por Hewlett-Packard, IBM y Seagate. Existen diferentes especificaciones de los niveles de cinta LTO, los cuales se denominan LTO-1, LTO-2, LTO-3, etcétera.

Clave Contraseña digital que se utiliza para firmar documentos electrónicos a fin de garantizar su autenticidad.

Cliente Computadora de una red que utiliza los datos proporcionados por el servidor.

Cliente/Servidor Modelo para diseñar una red en el que el poder de cómputo se encuentra dividido entre un procesador del cliente y uno del servidor, lo que permite que cada uno lleve a cabo las tareas que mejor desempeña.

CNE Ingeniero NetWare certificado.

Compuerta Dispositivo que conecta dos redes a todos los niveles del modelo de red OSI. Un ejemplo es una compuerta de correo electrónico que transmite correo electrónico de una red a otra.

Concentrador Dispositivo que conecta múltiples dispositivos de usuario a una red. Algunas veces se le llama *hub*.

Conectividad por línea telefónica (DUN) Término de Microsoft para una conexión de red por línea telefónica a través de un módem.

Conector BNC Conector tipo bayoneta que se utiliza en las redes Ethernet 10-Base2 (Thin).

Conexión directa por cable Conexión serial (RS-232C) entre dos computadoras. Usted también puede hacer una conexión directa por cable entre dos computadoras que tengan equipo Ethernet mediante un cable de conexión RJ-45.

Consola Interfase administrativa de servidor de NetWare.

CSMA/CD Acceso múltiple de sensado de portadora con detección de colisiones. Método utilizado en las redes Ethernet que administra los paquetes en un segmento.

CSU/DSU Unidad del Canal de servicio/Unidad de servicio de datos. Dispositivo de hardware que sirve de interfase entre las señales de una red y las señales que se transportan a través de una conexión a la red pública, como una línea T-1.

Cuello de botella En un sistema complejo, la parte que limita la velocidad de trabajo en todo el sistema.

Cuenta En un servidor, definición de los servicios del servidor de un usuario. Un usuario no puede acceder a un servidor o a una red sin una cuenta válida.

DAT Cinta de audio digital. A menudo se utiliza en los dispositivos de respaldo de red.

Datagrama En una red IP, colección de datos de red junto con la información de dirección y encabezado asociados. También se llama *paquete*.

DBMS Sistema de administración de bases de datos. Generalmente, base de datos relacional.

Derechos de acceso Derechos que controlan qué puede o no puede hacer un usuario con un recurso de red en particular.

Difusión Transmisión en la red que se envía a todos los nodos de ella o de la subred.

Digital Método de señalización en el que todas las señales son binarias (solo 1 y 0).

Directorio Estructura en forma de árbol del sistema de archivos de un disco, contenedor lógico de archivos.

Dominio 1) En Internet, es una red identificada con un nombre, como yahoo.com. 2) En las redes Windows NT de Microsoft, es la unidad administrativa más pequeña de una red.

DS0 Línea telefónica básica.

DS1 Línea telefónica digital utilizada para aplicaciones tanto de voz como de datos. Un DS1 transporta hasta 1.544 Mbps de datos, divididos en 28 canales diferentes, o sea que transporta hasta 28 canales de voz. Con frecuencia se le llama *línea T-1.*

DS3 Línea telefónica digital que transporta hasta 44.736 Mbps de datos. A menudo se le llama *línea T-3.*

Encabezado Información de control transportada junto con un archivo o una unidad de datos de red, como un paquete.

Encuadernación Base de datos que contiene información de las cuentas y de seguridad de las redes Novell, versiones 4 y más antiguas.

Equipo de comunicación de datos (DCE) Extremo de una interfase RS-232C u otra conexión serial. El DCE y el DTE son análogos a los conectores "macho" y "hembra", en el sentido que se necesitan ambos tipos para efectuar una conexión. Vea *Equipo terminal de datos*.

Equipo en las instalaciones del cliente (CPE) Palabra que se utiliza en las compañías telefónicas para la interconexión de equipo ubicado en las instalaciones de una compañía.

Equipo terminal de datos (DTE) Extremo de una interfase RS-232C u otra conexión serial. Los dispositivos DTE se comunican solo con un dispositivo DCE y viceversa. Vea también *Equipo de comunicación de datos.*

Escritura retardada Método que se utiliza para escribir datos nuevos o modificados en los discos de un servidor de la red a fin de mejorar el desempeño total. Los datos que van a ser escritos se almacenan temporalmente en la memoria hasta que el sistema esté libre (o por un lapso de tiempo definido), en cuyo momento los datos se graban en el disco.

Espejeo de discos Método que se conoce también como RAID 1, que escribe datos en forma redundante en dos discos.

Espina dorsal Cable común compartido por los diferentes segmentos de la red. A menudo, la porción de la espina dorsal de una red funciona a una velocidad más alta que la de los segmentos individuales, puesto que ésta tiene que transportar la mayor parte del tráfico de todos los segmentos conectados.

Ethernet Estándar de red que utiliza métodos CSMA/CD para transportar datos de red a través de diferentes tipos de medios de transmisión a velocidades diferentes.

EtherTalk Protocolo Apple para conectar computadoras Macintosh a una red Ethernet.

Fast Ethernet Red Ethernet que opera a 100 Mbps.

FAT Tabla de localización de archivos. Tabla que utilizan algunos sistemas operativos para asignar espacio para archivos en discos físicos.

Firewall Dispositivo de red que la protege de los intrusos externos.

Firma digital Código de autentificación incrustado en un mensaje de red.

Frame relay Servidor de telecomunicaciones que transporta datos asíncronos entre dos puntos de una WAN. Por eficiencia, el frame relay no lleva a cabo la detección y corrección de errores, pues deja esta tarea al software que se encuentra en los dos puntos que se desea conectar.

Full-duplex Conexión en la que ambos extremos pueden transmitir y recibir de manera simultánea.

Gb Abreviatura de *gigabit*, o mil millones de bits.

GB Abreviatura de *gigabyte*, o mil millones de bytes.

GHz Abreviatura de *gigahertz*, o mil millones de ciclos por segundo.

Half-Duplex (Simplex) Conexión en la que sólo un extremo puede transmitir a la vez.

HTML Lenguaje de marcado de hipertexto. Lenguaje de formateo utilizado para páginas web.

HTTP Protocolo de transferencia de hipertexto. Protocolo de red que se utiliza para acceder a páginas de un servidor de web.

Hub Dispositivo de red que conecta nodos múltiples a un segmento de red.

IEEE Instituto de Ingenieros en Electricidad y Electrónica. Asociación que define estándares para los aparatos eléctricos.

Ingreso Proceso para proporcionar información acerca de la cuenta y autentificación (como una contraseña) a una computadora o red a fin de obtener acceso a sus recursos.

Interfase a velocidad básica (BRI) Paquete de servicios ISDN que incluye dos canales del cliente a 56 ó 64 Kbps cada uno (64 Kbps es común en Estados Unidos), más un solo canal de datos que transporta 16 Kbps. A menudo, al BRI se le conoce como 2B+D.

Interfase común de compuerta (CGI) Estándar de programación que conecta las bases de datos y los navegadores de red.

Interfase de datos LAN por fibra óptica que trabaja a 100 Mbps, distribuidos por fibra (FDDI)

Internet Red pública mundial de servicios para negociantes y consumidores.

Intranet Modelada específicamente para una compañía después de Internet.

IPv6 Protocolo de Internet versión 6, que incrementa, en forma dramática, el número de direcciones disponibles e incluye otras mejoras al protocolo IP.

IPX Protocolo de red que se utiliza en las redes NetWare.

IRQ Línea de solicitud de interrupción. Switch ubicado en el hardware de una computadora que permite que un dispositivo envíe una señal al procesador.

ISDN Red Digital de Servicios Integrados. Estándar de telecomunicaciones que proporciona servicios telefónicos digitales a los negocios y a los consumidores.

ISO Organización Internacional de Estándares. Organización que define muchos estándares de computadoras, incluyendo los de conectividad de redes.

ISP Proveedor de servicios de Internet. Compañía que proporciona servicios de Internet directamente a los negocios y/o consumidores.

Java Lenguaje de programación que se deriva del lenguaje C, que permite la automatización de las páginas web de Internet.

Kb Abreviatura de *kilobit*, o 1 024 bits.

KB Abreviatura de *kilobyte*, o 1 024 bytes. KB representa 1 024 bytes en lugar de 1 000 bytes debido a que 1 024 es el número del exponente (potencias de 2) más cercano.

LAN Red de área local. Red específica de un edificio.

LAN manager Sistema operativo de red de Microsoft antiguo.

Línea privada Conexión telefónica dedicada siempre disponible.

Lista de control de acceso (ACL) Lista de permisos de seguridad para los archivos, directorios y otros recursos del servidor de Windows. Las listas de control de acceso también se utilizan con otros dispositivos y, en esencia, son listas de quién puede acceder a qué.

LocalTalk Sistema de conectividad de redes Apple para conectar impresoras Macintosh y Apple por medio de una red de baja velocidad (230 Kbps) mediante par trenzado.

MAC Control de acceso al medio. Subcapa (capa 2) del modelo OSI de conectividad de redes. Las redes IEEE 802.x dividen la capa 2 en la capa MAC y la capa de control del enlace lógico (LLC). El software de la subcapa MAC es único para todos los diferentes tipos de medio de transmisión de la red. En otras palabras, el software de la subcapa MAC de Thin Ethernet es diferente al software utilizado en la red Token Ring con par trenzado.

Mapeo de controladores Método que utiliza un directorio de la red para simular una letra de controlador local (como F: o G:) de una computadora cliente.

Mb Abreviatura de *megabit*, o aproximadamente un millón de bits. En general, se utiliza para velocidades de 100 Mbps o 100 millones de bits por segundo.

MB Abreviatura de *megabyte*, o 1 048 576 bytes.

MCSA Administrador de sistemas certificado por Microsoft. Subconjunto de requerimientos para la certificación MCSE que se orienta hacia los administradores de redes.

MCSE Ingeniero de sistemas certificado por Microsoft. Persona que ha aprobado un conjunto de exámenes administrados por Microsoft para certificarla como ingeniero en conectividad de redes.

MHz Abreviatura de *megahertz*, o un millón de Hertz (señales por segundo). A grosso modo, equivale a Mbps (millones de bits por segundo).

MIME Extensión de correo multipropósito por Internet. Estándar para la conexión de datos binarios (conexiones) a mensajes de correo electrónico por Internet. Está también disponible como S/MIME, que es una forma segura de MIME.

Módem Modulador/Demodulador. Dispositivo que permite que las señales digitales viajen a través de una línea telefónica analógica. En cada extremo de la conexión se requiere un módem.

MSAU Unidad de acceso multi-estación. Hub que se utiliza para conectar nodos Token Ring entre sí.

Multiplexaje Técnica que permite que múltiples señales sean agregadas a un canal de control.

Multiprocesador Computadora, sistema operativo o aplicación que utiliza más de un procesador para hacer su trabajo.

Navegador Aplicación que interpreta y despliega información formateada utilizando el lenguaje de marcado de hipertexto (HTML) en la web.

Programa de Ingreso Conjunto de comandos que corren de manera automática cuando un usuario ingresa a la computadora o a la red.

Protocolo de autentificación de saludo comprometido (CHAP) Estándar de comunicación de Internet para validar contraseñas encriptadas.

Protocolo de transferencia de archivos (FTP) 1) Protocolo de Internet para copiar archivos entre dos computadoras. 2) Programa que utiliza el protocolo FTP para hacer su trabajo.

Protocolo para la resolución de direcciones (ARP) Protocolo que determina una dirección de control de acceso al medio (MAC), a partir de dirección de Protocolo Internet (IP).

Puente Dispositivo de conectividad de redes que conecta dos redes entre sí utilizando las capas 1 y 2 del modelo OSI.

Punto de estancamiento Situación en la que dos computadoras o dos procesadores intentan acceder a un recurso de manera simultánea y esperan indefinidamente a que el otro termine de utilizarlo.

Respaldo completo Proceso mediante el cual todos los archivos de un controlador de red se copian en una cinta o en otro medio. El bit de archivo de cada archivo es puesto a cero como parte del respaldo completo.

Respaldo diferencial Respaldo que copia todos los archivos con su bit de archivo activado y no lo restablece cuando termina.

Respaldo generacional Metodología de intercambio de cinta que proporciona una buena granularidad de recuperación sin tener que consumir muchas cintas. También se le llama método abuelo/padre/hijo.

Respaldo incremental Método para respaldar archivos que tienen su atributo archivo en estado activo y después los desactiva.

Saludo Negociación de una conexión y de la transmisión de datos entre dos dispositivos.

Servidor de archivos Dispositivo de red primordialmente responsable del almacenamiento, compartición y acceso de archivos de los clientes de red.

Sistema de nombre de dominio (DNS) Sistema de Internet que convierte los nombres de dominio en direcciones IP.

T-1 fraccional Conexión de telecomunicaciones T-1 en la que solo algunos canales se rentan para su uso.

Trama Unidad de transmisión de la capa de enlace de datos en el modelo OSI de la red. Las tramas pueden ser de longitud variable.

Velocidad Velocidad a la que se transporta una señal analógica. La velocidad **en bauds** es análoga a los bits por segundo (bps). Por lo tanto, 2 400 bauds es, a grosso modo, equivalente a 2 400 bps.

Verificación de redundancia cíclica (CRC) Método para detectar errores en la transmisión y el almacenamiento de datos.



ÍNDICE

Las referencias a las figuras están en itálicas.



A



B



C

D

E



F



G



H



I



J



K



L



M

 N

 O

 P



Q



R

S

T

U



V



W



X



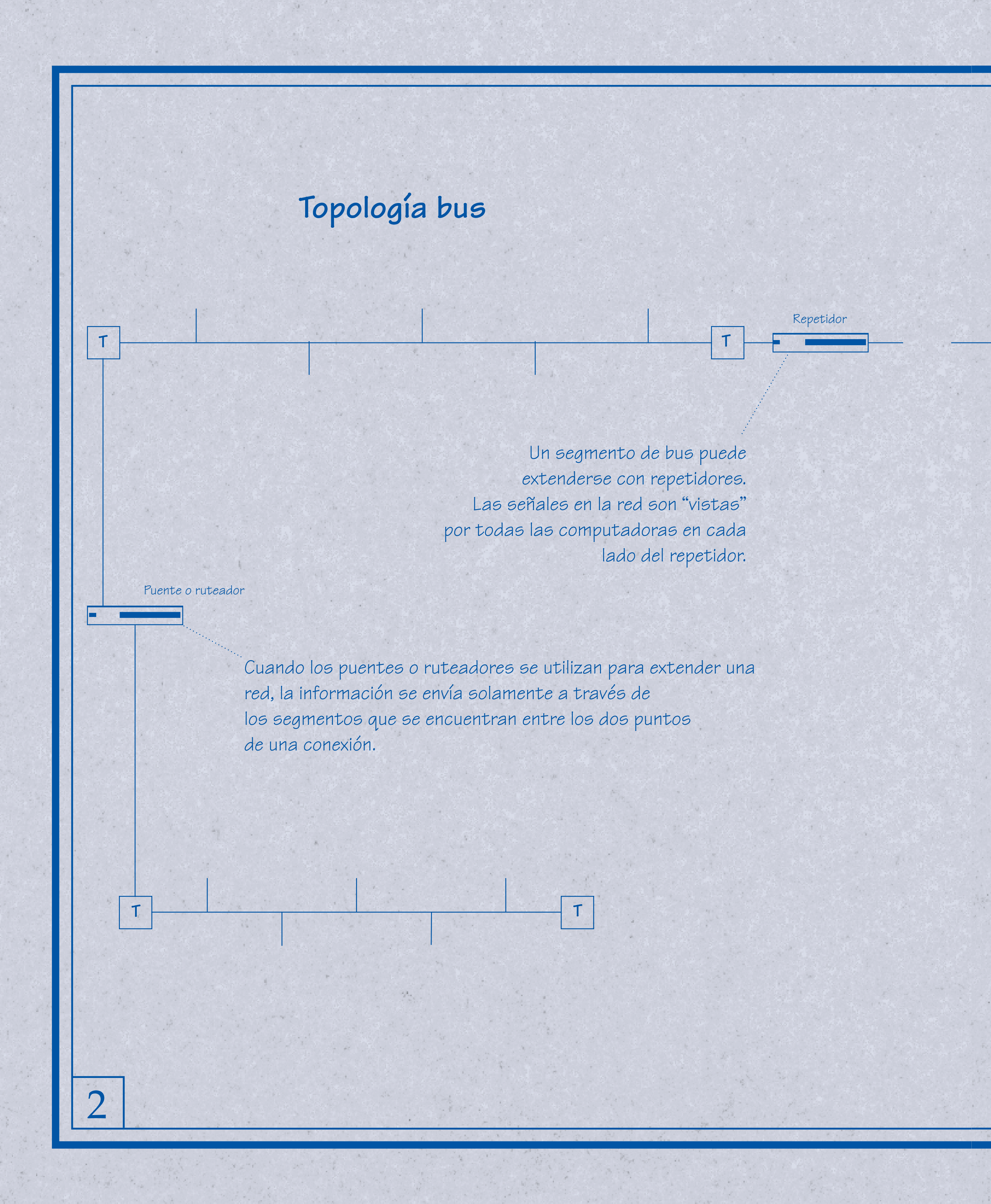
Z

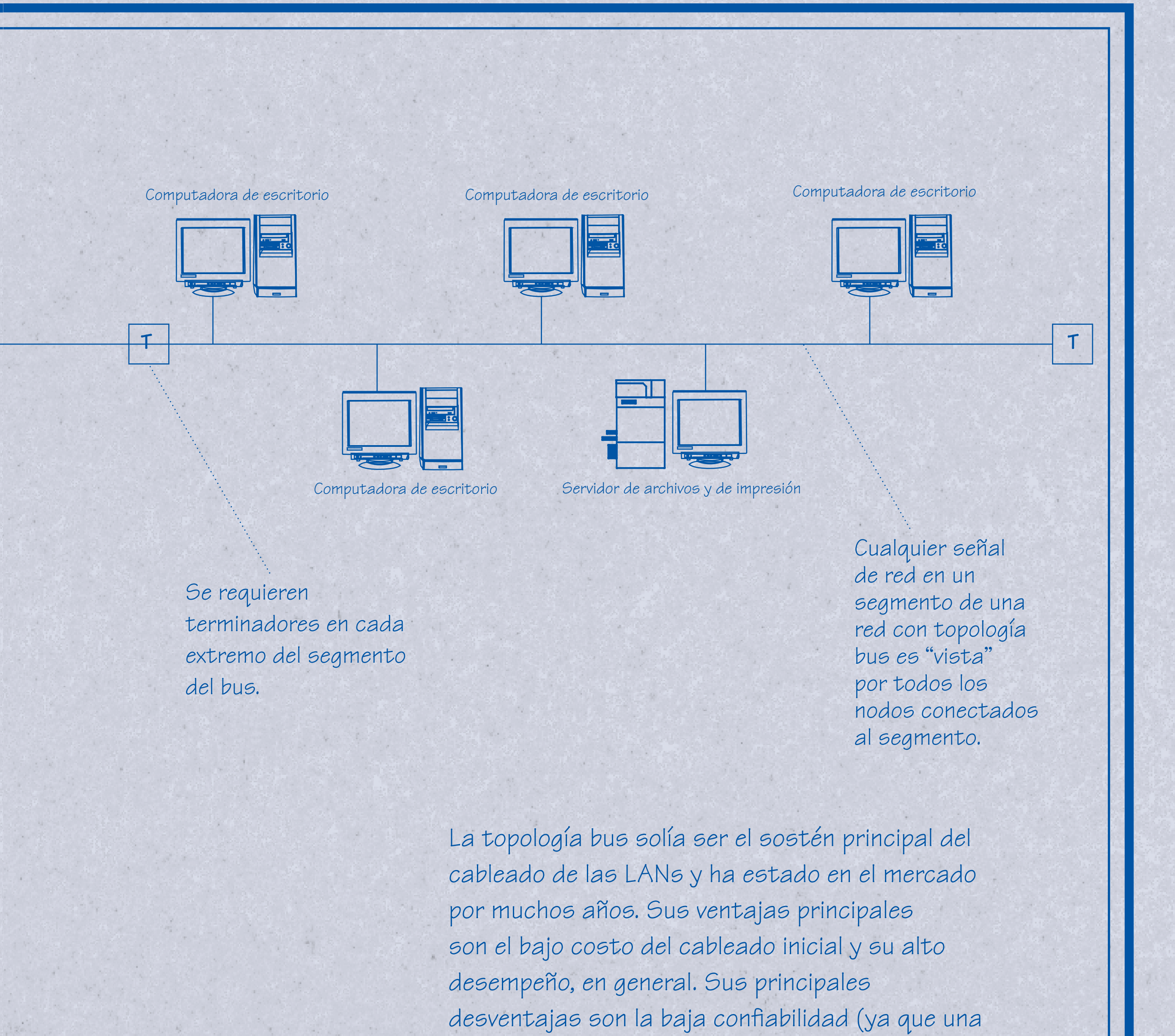
Para dominar el área de la administración de redes de computadora, usted necesita desarrollar la habilidad de visualizar qué está haciendo la red en cualquier momento. Este tipo de visualización es esencial en la administración de la red.

Por ejemplo, el concepto de la tecnología CSMA/CD de Ethernet puede visualizarse como una porción (en realidad, un paquete) de datos que ingresa al cable, viaja a través de él y, después, es recibido en el otro extremo. En realidad, la señal eléctrica llega al servidor a la velocidad de la luz y la recepción comienza en el destino antes de que la estación de trabajo que envió el paquete termine la transmisión. Sin embargo, la visualización de los "pedazos" de información puede ser esencial para comprender qué pasa, por ejemplo, dos estaciones de trabajo envían paquetes que sufren una colisión. La visualización le proporciona analogías con las que podría entender las redes y reparar los problemas de la red. De hecho, los mejores profesionales de las redes visualizan lo anterior de manera intuitiva.

Los siguientes planos ilustran algunas topologías básicas de red. Usted puede utilizarlos como punto de partida a fin de construir sus propias imágenes visuales de cómo funcionan las redes. Conforme lea el libro, piense en otras formas de visualizar los conceptos acerca de la conectividad de redes, como las configuraciones del hardware.

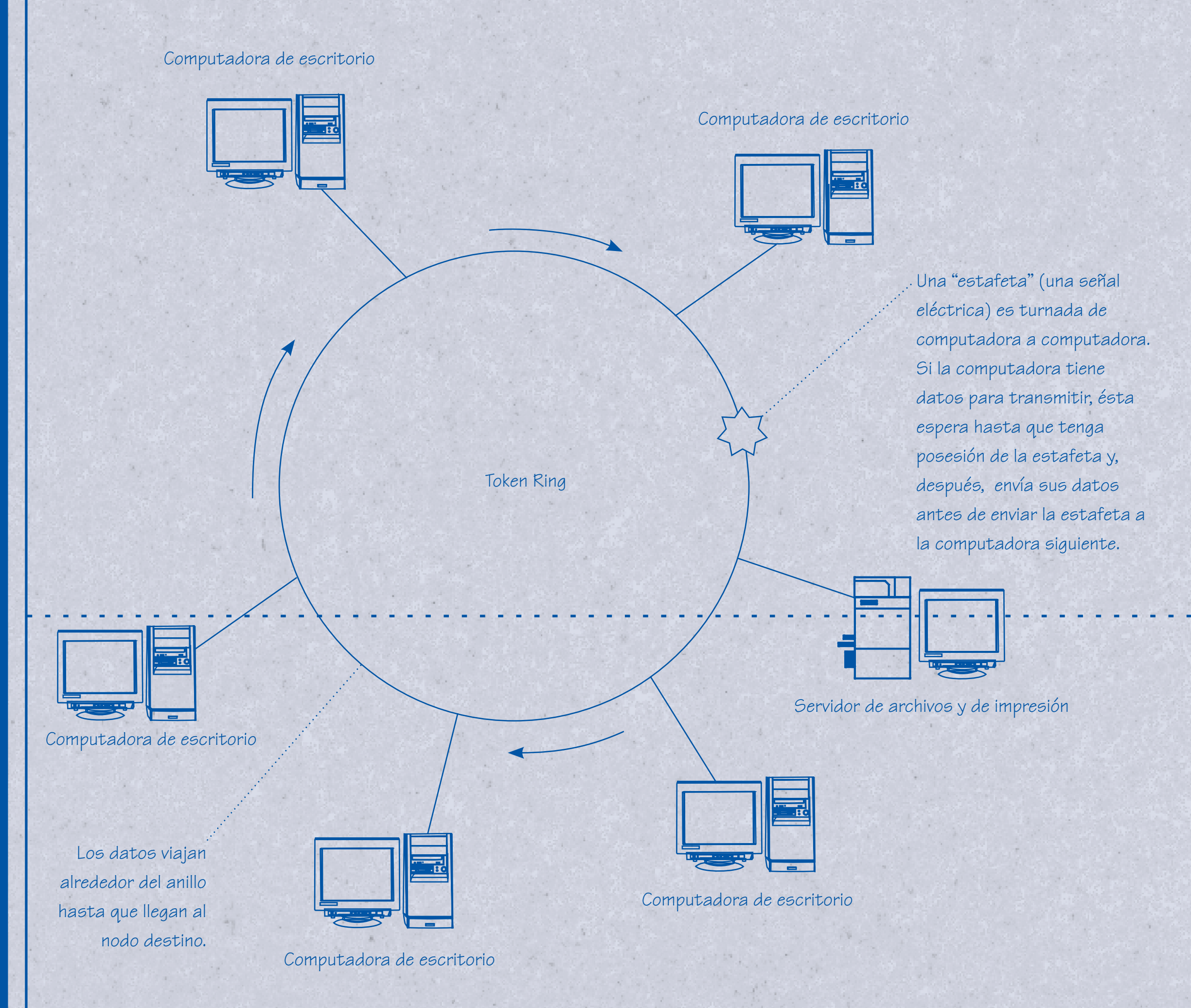
Topología bus





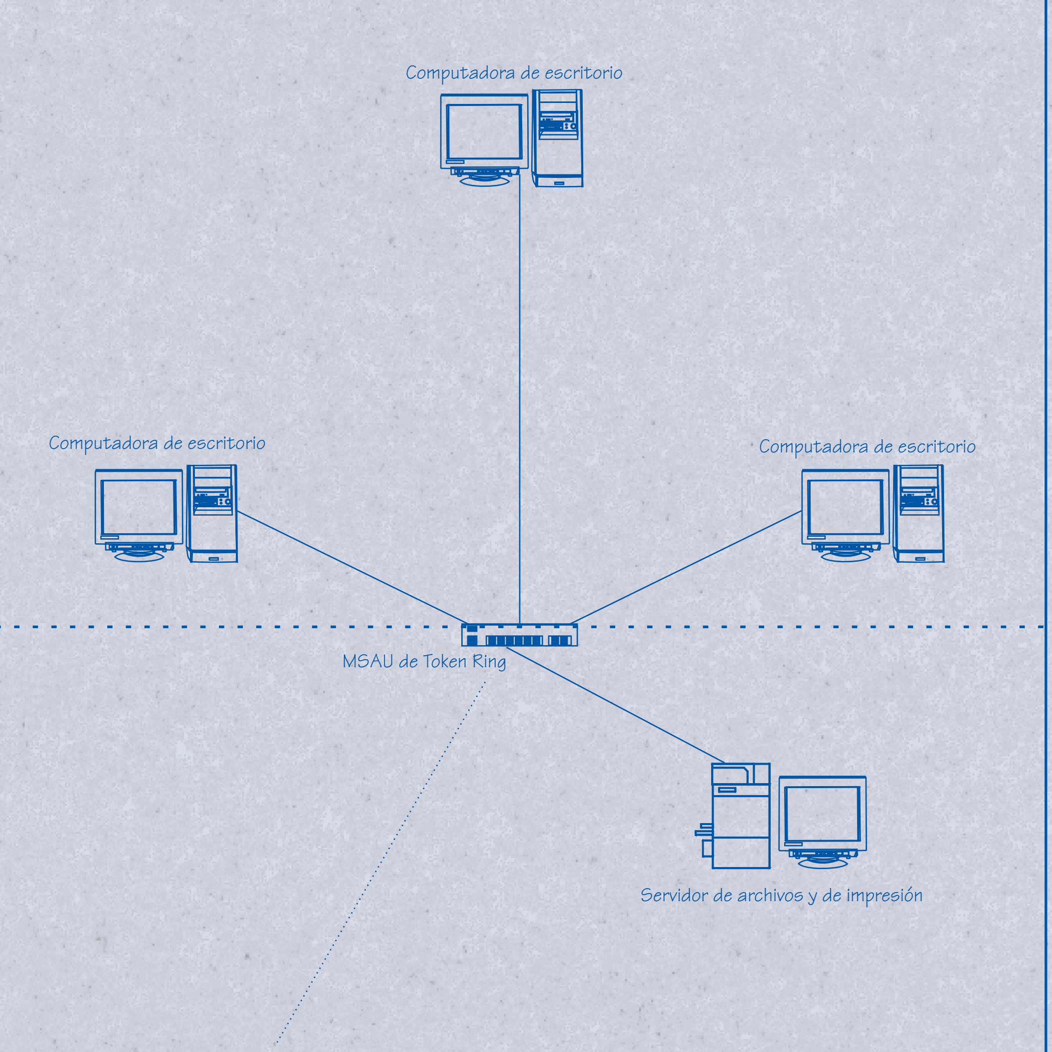
La topología bus solía ser el sostén principal del cableado de las LANs y ha estado en el mercado por muchos años. Sus ventajas principales son el bajo costo del cableado inicial y su alto desempeño, en general. Sus principales desventajas son la baja confiabilidad (ya que una ruptura en un punto de cualquier segmento saca de funcionamiento al menos un segmento completo) y la gran dificultad que existe para balancear el tráfico de la red en los diferentes segmentos.

Topología en anillo: vista lógica

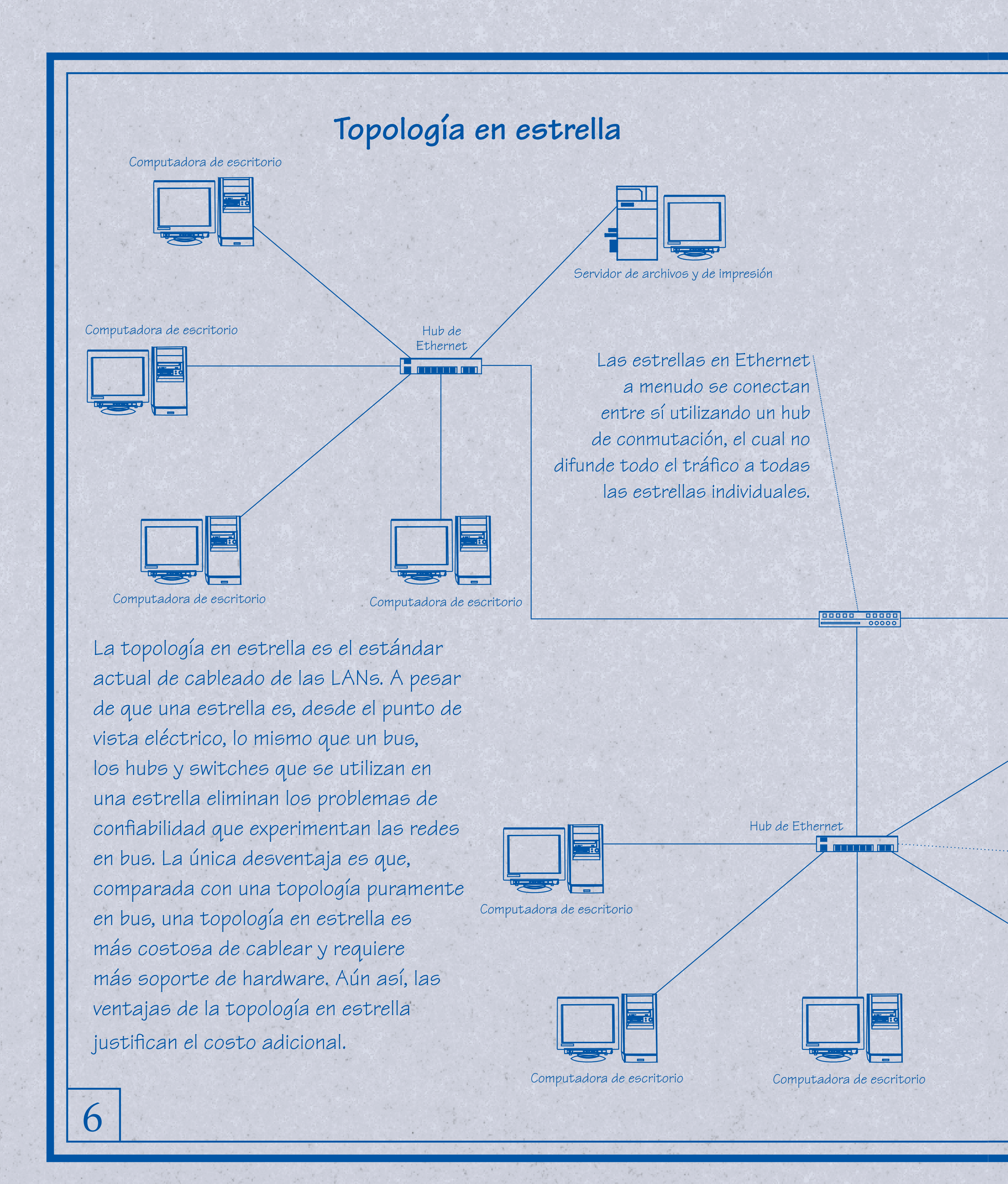


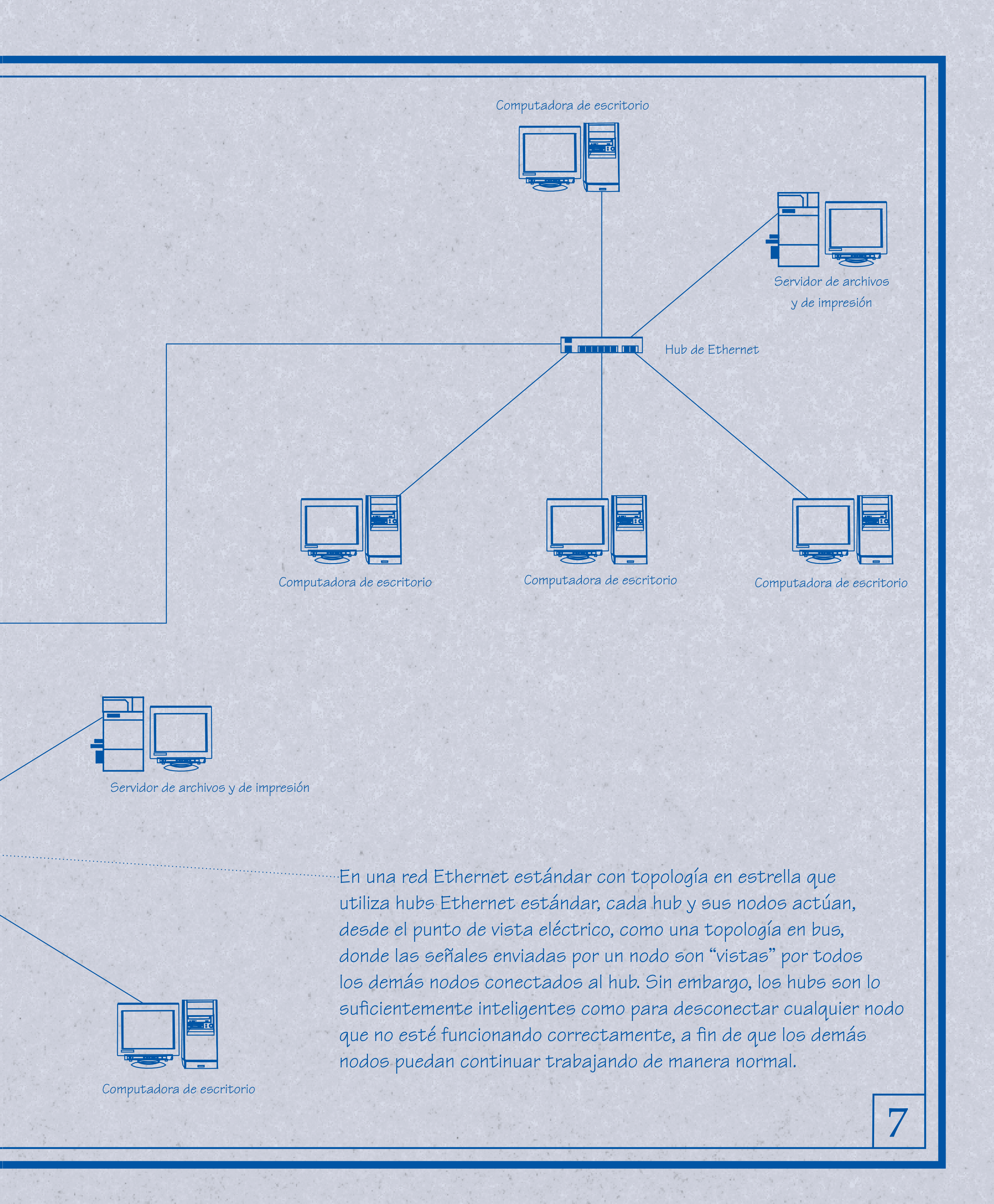
La topología en anillo se utiliza comúnmente en las redes Token Ring. Sus ventajas principales son la alta confiabilidad en comparación con las redes de topología en bus y una mayor capacidad para predecir y manejar cargas de tráfico muy variables. Su desventaja principal es que, en general, es más lenta que las topologías tipo bus y anillo basadas en Ethernet.

Topología en anillo: vista física

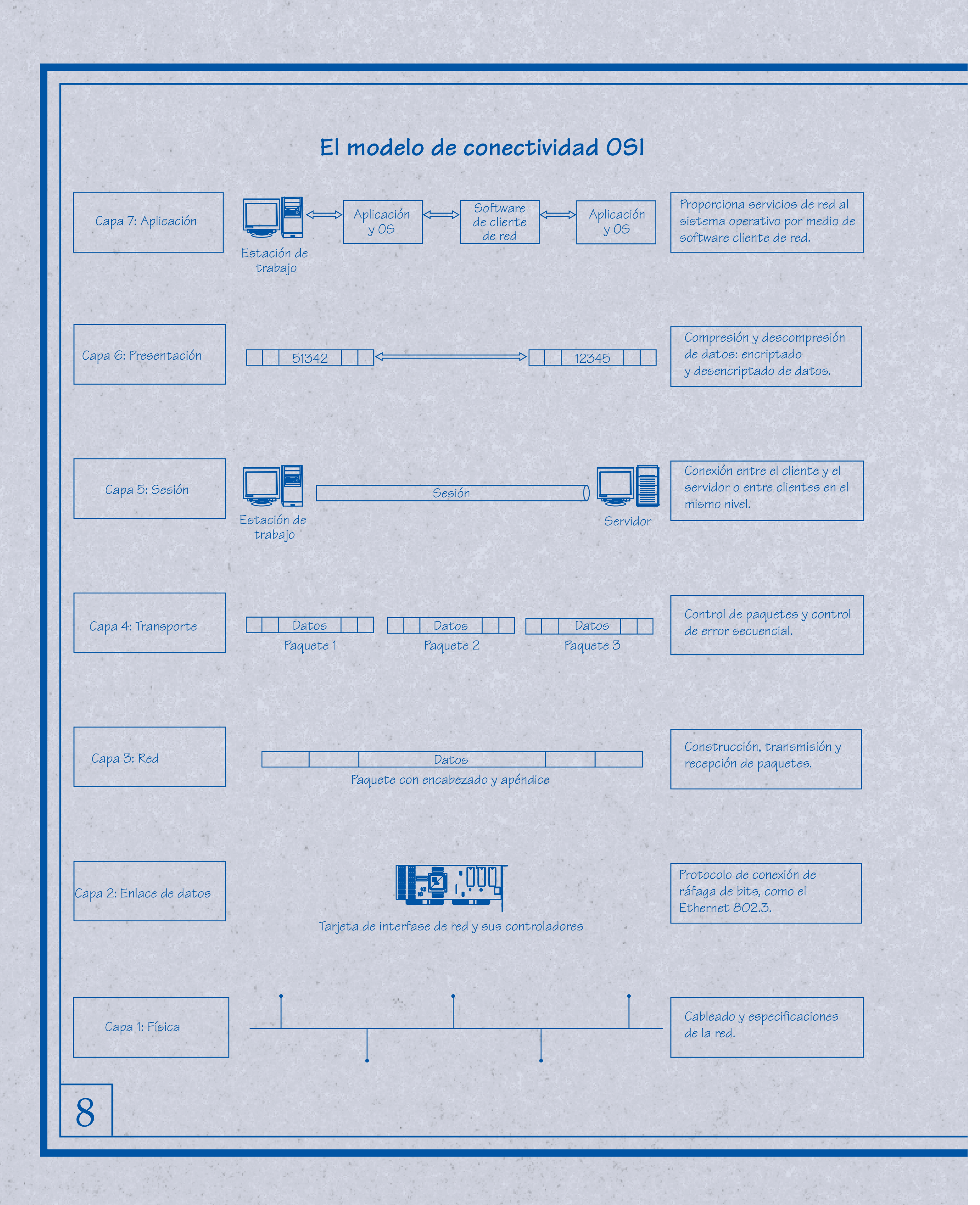


Mientras que las topologías en anillo son, desde el punto de vista eléctrico, un anillo, están cableadas en estrella, donde el cable de red de cada computadora está instalado hacia la unidad central MSAU.


Topología en estrella
Computadora de escritorio
Servidor de archivos y de impresión
Computadora de escritorio
Hub de Ethernet
Las estrellas en Ethernet a menudo se conectan entre sí utilizando un hub de conmutación, el cual no difunde todo el tráfico a todas las estrellas individuales.
Computadora de escritorio
Computadora de escritorio
La topología en estrella es el estándar actual de cableado de las LANs. A pesar de que una estrella es, desde el punto de vista eléctrico, lo mismo que un bus, los hubs y switches que se utilizan en una estrella eliminan los problemas de confiabilidad que experimentan las redes en bus. La única desventaja es que, comparada con una topología puramente en bus, una topología en estrella es más costosa de cablear y requiere más soporte de hardware. Aún así, las ventajas de la topología en estrella justifican el costo adicional.
Hub de Ethernet
Computadora de escritorio
Computadora de escritorio
Computadora de escritorio
6



En una red Ethernet estándar con topología en estrella que utiliza hubs Ethernet estándar, cada hub y sus nodos actúan, desde el punto de vista eléctrico, como una topología en bus, donde las señales enviadas por un nodo son "vistas" por todos los demás nodos conectados al hub. Sin embargo, los hubs son lo suficientemente inteligentes como para desconectar cualquier nodo que no esté funcionando correctamente, a fin de que los demás nodos puedan continuar trabajando de manera normal.



El modelo de conectividad OSI
Capa 7: Aplicación
Estación de trabajo
Aplicación y OS
Software de cliente de red
Aplicación y OS
Proporciona servicios de red al sistema operativo por medio de software cliente de red.
Capa 6: Presentación
51342
12345
Compresión y descompresión de datos: encriptado y desencriptado de datos.
Capa 5: Sesión
Estación de trabajo
Sesión
Servidor
Conexión entre el cliente y el servidor o entre clientes en el mismo nivel.
Capa 4: Transporte
Datos
Paquete 1
Datos
Paquete 2
Datos
Paquete 3
Control de paquetes y control de error secuencial.
Capa 3: Red
Datos
Paquete con encabezado y apéndice
Construcción, transmisión y recepción de paquetes.
Capa 2: Enlace de datos
Tarjeta de interfase de red y sus controladores
Protocolo de conexión de ráfaga de bits, como el Ethernet 802.3.
Capa 1: Física
Cableado y especificaciones de la red.
8